KEYWORD: Security Violations: Personal Conduct

DIGEST: Applicant, with several years of experience handling classified information, gave communications security (COMSEC) hardware loaded with material classified secret to an employee at work in June 2001 without verifying this person's clearance or need-to-know. In February 2002, Applicant loaded secret information onto a work computer that had not been approved for the storage of classified information and then sent the file over an unencrypted (unclassified) intranet at work. In May 2002, Applicant failed to properly document the receipt of a classified fax before shredding it in an unapproved shredder. His pattern of gross negligence in the handling of classified information is not mitigated where he continues to make excuses for his noncompliance with security regulations. Clearance is denied.

CASENO: 02-28059.h1

DATE: 03/30/2006

DATE: March 30, 2006

In Re:

SSN: ----------

Applicant for Security Clearance

ISCR Case No. 02-28059

DECISION OF ADMINISTRATIVE JUDGE

ELIZABETH M. MATCHINSKI

APPEARANCES

FOR GOVERNMENT

Daniel F. Crowley, Esq., Department Counsel

FOR APPLICANT

Jack K. Merrill, Esq.

SYNOPSIS

Applicant, with several years of experience handling classified information, gave communications security (COMSEC) hardware loaded with material classified secret to an employee at work in June 2001 without verifying this person's clearance or need-to-know. In February 2002, Applicant loaded secret information onto a work computer that had not been approved for the storage of classified information and then sent the file over an unencrypted (unclassified) intranet at work. In May 2002, Applicant failed to properly document the receipt of a classified fax before shredding it in an unapproved shredder. His pattern of gross negligence in the handling of classified information is not mitigated where he continues to make excuses for his noncompliance with security regulations. Clearance is denied.

STATEMENT OF THE CASE

On December 28, 2004, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to the Applicant which detailed reasons why DOHA could not make the preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for the Applicant. (1) DOHA recommended referral to an administrative judge to determine whether his clearance should be granted, continued, denied, or revoked. The SOR was based on security violations (Guideline K) and personal conduct (Guideline E).

On January 28, 2005, Applicant filed a *pro se* response to the SOR and requested a hearing before a DOHA administrative judge. On July 11, 2005, I issued a notice scheduling the hearing for August 22, 2005. At the hearing convened on August 22, 2005, Applicant was granted a continuance due to the unavailability of legal counsel. (2) On September 6, 2005, counsel for Applicant formally entered his appearance, and the following day, I scheduled a hearing for September 26, 2005.

At the hearing, seven government exhibits and three Applicant exhibits were admitted and testimony was taken from three witnesses in addition to the Applicant, as reflected in a transcript received on October 11, 2005. Also, at the government's request, I agreed to take administrative notice of pertinent sections of the National Industrial Security Program Operating Manual (NISPOM).[(3)]

FINDINGS OF FACT

DOHA alleged under Guideline K and Guideline E that Applicant violated his employer's and the government's regulations and procedures for the handling and safeguarding of classified information, in that he: 1) transferred custody of COMSEC hardware loaded with secret KYK material in June 2001 without first verifying the recipient's clearance and need-to-know; 2) improperly loaded secret material on an unclassified work computer and forwarded it via the company's unencrypted local area network to a coworker in February 2002; and 3) failed to record the receipt of a classified facsimile before shredding it in ay 2002. Applicant was also alleged under Guideline E to have falsified his April 2002 security clearance application in failing to disclose that he had been charged with a civil rights violation in April 1996.

In his pro se response, Applicant admitted the security violations but attributed the June 2001 and May 2002 incidents to poor training and/or the lack of proper procedures for the situations. Applicant acknowledged he had sent the classified data over the company's internal unclassified network, as he had not recalled that the data had become classified. Applicant offered in mitigation that he had worked diligently since the incidents to improve his security posture and to implement better security guidelines at his facility. As for the omission from his SF 86 of the civil rights complaint, Applicant indicated that his family's rights were infringed as "publicly confirmed by a Judge," he assumed it was not necessary to report the charge. At his hearing, Applicant challenged whether his transfer of the custody of the COMSEC hardware to a cleared coworker was a violation of established security procedure. After a thorough review and consideration of the evidence of record, I make the following findings of fact:

Applicant is a 48-year-old principal electrical engineer employed by the same defense contractor (company A) since June 1980 on the award of his bachelor's degree. He seeks to retain the secret-level security clearance that he has held since about October 1980.[(4)]

From July 1982 to July 2000, Applicant lived in two-family dwelling adjacent to a local park. He and his mother shared one apartment. Relations bearing the same last name resided in the other. Starting in November 1992 and continuing to July 1996, the family contacted the police on numerous occasions complaining of ongoing vandalism of their cars and home, violation of park rules (youths over age 12 playing baseball in the park, noise and fireworks in the park), and trespass onto their property.[(5)] In August 1996, the local police filed a civil rights violation against Applicant and a female relation residing in the other apartment. Applicant filed a motion to dismiss on the basis the police had not set

out the particulars of any crime. In August 1997, the charge was dismissed without prejudice. Applicant did not report the charge on a security clearance application (SF 86) he subsequently executed on April 29, 2002, as he viewed the dismissal as a vindication and mistakenly thought it did not have to be reported.

Applicant has spent the last 13 years working on a program for the U.S. military involving a satellite system. Having worked on every aspect of the program in terms of hardware, Applicant handled classified information on a regular basis and received annual security refresher briefings, COMSEC training, and classified custodian briefings. While assigned to a secure test and integration facility in June 2001, Applicant borrowed COMSEC hardware loaded with keying material classified secret (hereinafter "KYK") from an engineer working on a different military program. Applicant did not have access to the secured container where the KYK was kept. Unable to find this engineer when he went to return it, Applicant gave the KYK to a technician, who promised to secure it. Applicant believed this employee had the requisite clearance and made no effort to verify his clearance or need-to-know. This technician had been cleared for secret access since at least December 1992, COMSEC briefed since January 1993, and had a need-to-know. He placed the KYK in his locked desk and forgot to secure it. The engineer from whom Applicant had borrowed the KYK discovered it was missing from the safe while conducting end-of-day checks late that evening. Asked about the KYK's whereabouts, Applicant indicated he had given the KYK to one of the technicians, but he could not recall this employee's name.[(6)] Early the next morning, the test site manager, after speaking with Applicant, determined who the technician was, and the still loaded KYK was recovered from the technician's locked desk.

Company A's COMSEC custodian reported the incident to the company's security manager and to the government agency with oversight over COMSEC. Since the loaded fill device was stored overnight in a locked desk located in a closed area of the facility secured by perimeter controls, alarms, video surveillance, and hourly patrol guards, the incident was evaluated as "No Compromise." All parties involved, including Applicant, were rebriefed as to the proper safeguarding of the classified loaded fill devices, and the need to notify the COMSEC custodian immediately of suspected incidents. Applicant was verbally reprimanded by his supervisor for failure to ensure that other parties with accountability responsibility were informed of the change of custody and informed that he could face suspension in the event of another security incident.

In mid-February 2002, while very busy preparing for flight testing, Applicant was asked by a coworker for a portable data recorder (PDR) file. Applicant downloaded from an approved classified automated information system an old PDR file that was classified secret and sent the secret document over company A's unencrypted local area network to the coworker, who held a secret clearance. The affected computers were located in a closed area of the facility. The coworker, who had saved the file to his hard drive, recognized on review that it contained classified material. He notified Applicant of its classified nature, and company security of the incident, and sanitization efforts were undertaken. In March 2002, Applicant was issued a security violation for his transmission of the secret email over the company's internal, unclassified network. Citing as well Applicant's "careless handling" of the COMSEC KYK in June 2001, a company security manager expressed concern over "a pattern of negligence that seems to be developing in regards to [Applicant's] handling of classified materials." While the likelihood of compromise was considered remote in both instances, Applicant was advised that further incidents could lead to serious adverse actions impacting his active security clearance status. He was also informed he would be required to participate in security awareness training.

On April 17, 2002, DSS was informed of the results of the company's administrative inquiry into the LAN

contamination and its assessment (concurred in by the information owner) that compromise could not be ruled out as all LAN contaminations are categorized as "lost" information. However, all containment and sanitization actions were considered adequate. On May 9, 2002, a DSS industrial security representative with cognizance over the facility conducted an investigation. In response to her concerns over whether Applicant intentionally breached security in the LAN contamination, the facility's information systems security manager interviewed Applicant, who indicated it was an honest mistake attributable to work-related stress. In follow-up to the DSS, the security manager expressed his belief that Applicant "did not intentionally load a classified file onto an unclassified resource to cause this contamination." (Ex. 4)

In May 2002, Applicant received secret documentation over a secure fax at the test integration site. He noted the document's receipt in the fax log located near the machine, but company procedures required all classified material be entered into receipt logs maintained by document control at another facility. After using the document, he destroyed it in a shredder in the local work area that was not approved for the destruction of secret information. The shredder bore no markings, neither a security classification nor a prohibition against use for destruction of classified material, and Applicant did not understand that this destruction was improper. This violation of NISPOM and company security practices did not result in a compromise of classified information. Applicant received a one-week suspension from work for his failure to follow security procedures. The DSS industrial security representative with cognizance over the facility submitted on July 19, 2002, an adverse information report to the Defense Industrial Security Clearance Office in accordance with the NISPOM, citing Applicant's "pattern of negligence in the handling of classified material" (three violations of security procedures over a period of less than 12 months). (Ex. 5)

After his suspension, Applicant was re-immersed in a secure environment where he handled classified information regularly. Applicant became proactive in educating himself about his security responsibilities. In September 2002, the company hired a new security manager at about the same time that it relocated Applicant's project to a new facility. Applicant assisted the new security manager with the design and implementation of security measures at the new facility, including an end-of-day security check program and media and equipment labeling. Shredders not approved for the destruction of classified information were labeled with the instruction to process no classified.

Applicant has not been found to be in violation of any security requirements.

On February 19, 2004, Applicant was interviewed by a DSS special agent about the three security violations. Concerning his transfer of custody of the COMSEC "KYK" to the technician in June 2001 (mistakenly reported by him as October 2001), Applicant expressed his belief that the technician had the proper clearance, so he was not certain why he was cited for not verifying the technician's clearance. While Applicant admitted he had received a COMSEC briefing, there were no clear procedures in place for the transfer of responsibility, so he did not believe his acts were wrong. Applicant acknowledged the improper transfer of classified material over unsecured lines to a coworker in February 2002 ("mistake on [his] part [that he] should have known not to do"), attributable to the file being previously unclassified and to him being overloaded with work. Applicant explained that on receipt of the classified fax in May 2002, he "logged it into the fax log, used it, locked it in [his] safe and eventually destroyed it." It was not clear to him that he was supposed to bring it to document control for shredding, and he cited poor security guidance/training. Acknowledging that he had received required briefings, Applicant opined they were not comprehensive or backed up by in-person classes or refresher meetings. Applicant volunteered that since the May 2002 violation, he had worked closely with security officials at the company in the creation of a new automated information system for the satellite project at their new location, and properly dispositioned classified material he inherited from other employees. He reported a drastic change for the better in the company's security department under the present security officials.

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 has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960). Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3.

Enclosure 2 of the Directive sets forth personnel security guidelines, as well as the 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 that the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Concerning the evidence as a whole, the following adjudicative guidelines are most pertinent to this case:

Security Violations. Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information. (¶ E2.A11.1.1)

Personal Conduct. 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. (¶ E2.A5.1.1)

CONCLUSIONS

Having considered the evidence of record in light of the appropriate legal precepts and factors, I conclude the government established its case with respect to Guideline K, security violations, and Guideline E, personal conduct, because of Applicant's noncompliance with security regulations. Applicant was involved in three security incidents between June 2001 and May 2002 in violation of his obligation under the NISPOM to safeguard classified information entrusted to him (NISPOM ¶ C5.1.1, ¶ 5-100 Jan. 1995 NISPOM).

In June 2001, Applicant transferred custody of a COMSEC KYK to a technician without first verifying this employee's clearance level and need-to-know. While no compromise occurred in the transfer as this technician had the appropriate clearances, Applicant did not have sufficient familiarity with this technician or his work to know that this technician was cleared to receive the classified loaded fill device. Applicant and this technician worked on different projects, and Applicant could not identify this technician by name when asked about the missing KYK. Applicant now claims to have known the technician "for many, many, many years," and that he has a problem with names (Tr. 138-39). Had Applicant a close working relationship with this technician where he would reasonably have known of the technician's duties, it is unlikely Applicant would have forgotten his name or been verbally reprimanded by his supervisor for turning over the KYK without verifying the technician's clearance.

Then in February 2002, Applicant downloaded a secret PDR onto a floppy disk, and then sent it via his unclassified work computer over the company's unsecured internal network to a coworker, in violation of ¶ C8.1.1.1. of the NISPOM (¶ 8-100 Jan. 1995 NISPOM), which requires that computer and networking systems be operated so that the information is protected against unauthorized disclosure of classified information, loss of data integrity, and to ensure the availability of the data and system. He was assessed a security violation in March 2002 for the automated information system (AIS) violations.

Only a few months later, Applicant failed to comply with the NISPOM's requirements and his employer's DSS-approved procedures for the control (¶ C5.2.3., ¶ 5-202 Jan. 1995 NISPOM) and disposition (¶ C5.7.1. et. seq., ¶ 5-700 et. seq. Jan. 1995 NISPOM) of classified material. In May 2002, Applicant improperly documented receipt of a classified fax by entering it only on the fax log and failing to ensure that it was documented in external classified receipt records maintained by his employer. After using the document, he destroyed it in a shredder not approved for the destruction of classified material.[(7)]

While Applicant did not set out to violate security practices, he chose expediency over his security responsibilities during an extremely busy flight test period that required "constant handling of classified materials during long and unpredictable work shifts." (*See* Tr. 174) Under Guideline K, disqualifying condition E2.A11.1.2.2. *Violations that are deliberate or multiple or due to negligence*, applies. The government made its case for E2.A11.1.2.1. *Unauthorized disclosure of classified information* as well because of the LAN contamination in February 2002, which is considered a compromise. Under Guideline E, disqualifying conditions E2.A5.1.2.1. *Reliable, unfavorable information provided by associates, employers, coworkers . . .* , and E2.A5.1.2.5. *A pattern of dishonesty or rule violations*, are apposite.

When viewed in the context of his several years of classified access before June 2001, his failure to comply with security requirements over the 2001/02 time frame is infrequent (*see* MC E2.A11.1.3.2. actions that were isolated or infrequent under Guideline K). Yet, in violating several different security requirements (failure to verify clearance, transfer of custody without accountability, loading of classified onto an unclassified computer, transmission of classified over unencrypted system, mishandling of a classified fax with destruction in an unapproved shredder), he exhibited a pervasive lack of judgment with regard to his security responsibilities.

Excepting the February 2002 transmission of the secret PDR over his employer's unencrypted LAN, Applicant attributes his violations to inadequate security measures or insufficient security education ("One of the things engineers have to be told is they have to be told what to do and what not to do, it's very important that clear and concise guidelines. And those types of bulletized reminders are very important to us, to have those posted and available. And at the old test site we just did not have those available." Tr. 143).While the record confirms improvement in the company's security posture since September 2002, Applicant had received annual refresher briefings as well as COMSEC and classified custodian briefings. The company's information systems security manager, who was involved in the administrative inquiry of the LAN contamination in 2002, expressed his belief that while Applicant did not intentionally commit the security violations, "he was certainly trained and should have known better." (Tr. 53)

As for specific deficiencies in security raised by the Applicant, while his employer may not have spelled out the procedure to follow in transferring custody of a KYK to another employee, Applicant was clearly aware of his fundamental obligation as a cleared employee to ensure that the classified KYK was appropriately safeguarded. Apart from the need-to-know issue, Applicant was accountable for the KYK in the absence of any notification to the original custodian that he had transferred custody. As for the February 2002 download of a secret document to a floppy, failure to be informed as to a specific trusted download procedure ("I felt I could have used more training on the trusted download procedure, because I did not have specific training in the trusted download procedure at the time." Tr. 151), does not adequately address his transmission of a secret document over an unencrypted network. Assuming the PDR had been unclassified in the past, he had an obligation to verify the document's classification before transmitting it over the unclassified LAN, especially where he obtained it from a classified AIS system. His coworker immediately recognized the document as classified, and all indications are that Applicant was not ignorant of its classified nature. When asked about the violations in February 2004, Applicant described it as "a mistake on [his] part." At his hearing, he testified, "If I had stopped to think about it maybe I wouldn't have done it at all because I would have thought about it and said, well that's a stupid thing to do . . ." (Tr. 162). While he later testified that he might have been confused about the classified nature of the document that day (Tr. 163), Applicant told the FSO in 2002 that he made a mistake by using the wrong computer, that he should have used the classified system. (Ex. 5)

The applicability of mitigating condition ¶ E2.A11.1.3.3. *Actions that were due to improper or inadequate training* is limited to his handling of the classified facsimile. Applicant testified, with no rebuttal from the government, that this was the only classified fax he had ever received. (Tr. 169) While he learned how to handle documents, "[he] did not have a specific procedure for faxing and receipt of faxes, nothing that said step one, two, three, do this, [he] did not have anything specific in writing." (Tr. 151) Applicant had logged the receipt of the classified fax in the record attached to the fax, and he apparently did not understand he had to notify document control, which was located offsite. The shredder he used to destroy the document was unmarked, but located in a closed area. Subsequent remedial measures taken by the company include the marking of equipment, including shredders. Yet, especially where it was the first time that he handled a classified facsimile, Applicant had an obligation to inquire of security whether there were any special requirements. His failure to inquire is especially troubling given his experience and the regularity with which he handled classified material.

The negative security implications of Applicant's mishandling of classified material are not reduced or diminished by the absence of malicious motives on Applicant's part or his cooperation with the investigations of those security violations. At the same time, security clearance determinations are not designed to punish wrongdoing, but involve an assessment of future security risk. Confirmed by the company security personnel who testified at the hearing, Applicant received "quite a bit of training" since the security incidents. (*See* Tr. 53). The security manager, whose hire coincided with the relocation of Applicant's group from the test integration site to its present facility, testified Applicant was one of a small group who "went the extra mile" to ensure compliance with security requirements, helping her with the new building's layout, a security end of day check program, attending to media and equipment labeling and other detailed administrative work, and "by offering solutions when a security requirement conflicted with an efficiency or operational condition, instead of merely complaining about the problem." (Tr. 173) She opined that in contrast to the typical employee found culpable of a security violation who maintains contact with the security office only at a level consistent with the general population, "[Applicant] went a step further by becoming a champion of good security practices within his own peer group and became a liaison to the local security organization." (Tr. 174)

Neither of the two company security professionals who testified at the hearing (the information security manager as a government witness) considers Applicant a risk to security based on his efforts to improve his security posture since 2002. MC E2.A11.1.3.4. *Demonstrate a positive attitude towards the discharge of security responsibilities*, applies, and there have been no subsequent violations of security. Whether or not Applicant has rehabilitated himself depends also on a recognition and acknowledgment of error, however, and Applicant's record in this regard is somewhat problematic. Despite all of his security training, he has not shown that he understands the concerns of the government with regard to his failure to verify the clearance and need-to-know of the employee to whom he turned over the KYK. He denies fault in that incident, citing the technician's actions as "the proximate cause" for not properly securing the KYK (*see* Ex. A). Applicant ignores the concern with respect to his own conduct, which was aptly summed up by the FSO in Exhibit A, to wit: "As a [sic] cleared employees, everyone must be cognizant over the accountability of classified materials." While his efforts to improve his security posture are viewed favorably, he has yet to take full responsibility for violations that he should have known better than to commit. For example, in the transmission of the secret PDR over an unclassified system, "I was running around doing my thing, so I did the transfer, I did not consider the compromise, that wasn't in my head . . . I might have been confused about it that day, because I know the PDR classification changed, it changed, we handled PDR for many years as unclassified." Tr. 162-63). SOR ¶¶ 1.a., 1.b., 1.c., and 2.a. are resolved against him.

Under Guideline E, the government also alleged the deliberate falsification of his April 2002 SF 86 for failing to list the civil rights violation charge stemming from complaints made to the police about trespassers and vandalism on his property, and prohibited ball playing in the adjacent park. Intentional concealment of the charge would fall within disqualifying condition E2.E2.A5.1.2.3. *Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination*. I am persuaded Applicant did not understand that it had to be listed, given the nature of the charge (civil rights violation), that it was in reaction to him complaining of conduct by others, such as the vandalism against his property, some of it substantiated by the responding police, and the charge was dismissed. SOR ¶ 2.b. is resolved in his favor.

FORMAL FINDINGS

Formal Findings as required by Section 3. Paragraph 7 of Enclosure 1 to the Directive are hereby rendered as follows:

Paragraph 1. Guideline K: AGAINST THE APPLICANT

Subparagraph 1.a.: Against the Applicant

Subparagraph 1.b.: Against the Applicant

Subparagraph 1.c.: Against the Applicant

Paragraph 2. Guideline E: AGAINST THE APPLICANT

Subparagraph 2.a.: Against the Applicant

Subparagraph 2.b.: For the Applicant

DECISION

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

Elizabeth M. Matchinski

Administrative Judge

1. The SOR was issued under the authority of Executive Order 10865 (as amended by Executive Orders 10909, 11328, and 12829) and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992 (as amended by Change 4).

2. The attorney had not formally entered his appearance, although Department Counsel confirmed the attorney intended to represent Applicant provided retainer arrangements and continuance of the August 22, 2005, hearing.

3. The government submitted for administrative notice extracts from the NISPOM dated January 1995, before its administrative reissuance in May 2000. Since all of the Guideline K allegations post-date Change 2 to the NISPOM, any section references to the NISPOM will be as enumerated in the May 2000 version. In a subsequent reissuance of the NISPOM dated February 28, 2006, the Department of Defense has returned to the numbering of the 1995 version.

4. Applicant testified to receiving his first clearance in 1990 when he started on his present program. (Tr. 127) His SF 86 (Ex. 1) indicates award of a secret clearance in October 1980.

5. A motion to dismiss a civil rights complaint filed against Applicant in August 1996 references 86 police reports obtained from the prosecution, most involving area youths playing baseball in the nearby park, trespassing on or vandalizing Applicant's property. (Ex. 3) Applicant was specifically identified as the caller in about seven of the reports (June 12, 1994, youth throwing stones and baseball at residence; June 15, 1994, youth hitting tennis ball in park, frustration with slow police response; July 16, 1994 coed group trespassing and throwing pears at home and cars (confirmed); September 2, 1994, truck parked nightly in prohibited zone; April 30, 1995, thud on home exterior related to youth baseball in park; May 19, 1996, rocks thrown at his home and car; July 6, 1996, overage youths (confirmed) playing baseball in park).

6. The COMSEC custodian reported on June 11, 2001, that when the KYK was discovered missing, Applicant indicated he had given it to a technician to return it to the safe, but Applicant was unable to recall the name of the technician. Early the next morning, Applicant was questioned by the test site manager, whereupon the technician's identity was determined. In subsequent correspondence to the DSS, the company's FSO referred to a statement which is not of record here that apparently confirms Applicant could not remember to whom he gave the KYK. (Ex. 4)

7. It is not clear whether the destruction was witnessed. Under ¶ C5.7.7. of the NISPOM (¶ 5-706 Jan 1995 NISPOM), one person is required to witness the destruction of secret and confidential material.