DATE: April 11, 1997

In re:

SSN:

Applicant for Security Clearance

ISCR OSD Case No. 96-0457

DECISION OF ADMINISTRATIVE JUDGE

ELIZABETH M. MATCHINSKI

APPEARANCES

FOR THE GOVERNMENT

Matthew E. Malone, Esq.

Barry M. Sax, Esq.

Department Counsel

FOR THE APPLICANT

Pro se

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) pursuant to Executive Order 10865 and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992, as amended by Change 3, issued a Statement of Reasons (SOR) dated October 18, 1996, 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 and recommended referral to an Administrative Judge to conduct proceedings and determine whether clearance should be granted, continued, denied or revoked.

A copy of the SOR is attached to this Decision and included herein by reference.

On November 9, 1996, Applicant responded to the allegations set forth in the SOR. By letter dated November 19, 1996, he requested a hearing. The case was assigned to the undersigned on a transfer due to workload considerations on January 15, 1997, and on January 16, 1997, a hearing was scheduled for February 13, 1997. At the hearing held as scheduled, seven Government exhibits and four Applicant exhibits were admitted into evidence. Testimony was taken from two Government witnesses and the Applicant. A transcript of the hearing was received by this office on February 24, 1997.

FINDINGS OF FACT

After a thorough review of the evidence in the record, and upon due consideration of same, this Administrative Judge renders the following findings of fact:

Applicant is a 40 year old ---------- who has worked for his current employer (company A) since

May 1995. He seeks to retain his Secret security clearance.

In February 1980, Applicant was hired as an ---------- by a defense contractor (company B) which was in the business of conducting Tempest testing of communications security (COMSEC) equipment and components. On February 13, 1981, Applicant was granted a Top Secret security clearance by the Defense Industrial Security Clearance Office which permitted him to begin working on classified Tempest test and evaluation programs.[(1)] Applicant received favorable performance reviews due to his technical expertise as a ----------.

In 1985, Applicant was given the opportunity to work on a very large systems integration program where he had both technical and program management responsibilities. Until 1989, company B's service contract was based on a fixed number of employees to perform Tempest test and analysis services. In 1989, the contract vehicle was modified to where Tempest test tasks were awarded on a time and material basis. Security services were no longer paid by the Government, but became an overhead cost. By the 1989/90 time frame, business had declined significantly to warrant downsizing through layoff and retirement of employees, to include the facility security officer (FSO). In October 1990, Applicant accepted a promotion, with an increase in pay, to the position of ---------- with concomitant additional responsibility as the FSO tasked with ensuring compliance with the Department of Defense Industrial Security Program. On becoming the FSO, Applicant was briefed by a Defense Investigative Service (DIS) Industrial Security Specialist (ISS) about the duties and responsibilities of the facility FSO.[(2)] Applicant took a "hands-off" approach to security at the facility, delegating all security related activities, to include briefings, managing classified documentation and equipment, dealing with visit requests, to two subordinates: co-worker C, who served as COMSEC custodian and security administrator, and co-worker D, an engineering technician who was security administrator and alternate COMSEC custodian until he left the employ of company B on December 13, 1993 when co-worker E (a laboratory technician who prior to that date served as alternate security officer) assumed his duties.[(3)]

As the -----/security manager, Applicant was required to submit weekly and monthly budget reports reflecting the amount of contract work performed compared to overhead work. Under pressure by the parent company to keep overhead expenses to a minimum and to eliminate time spent on non-contract work, Applicant instructed the security staff to spread out their security responsibilities throughout the year so as to avoid bunching manpower around DIS inspections of the facility. Although the intent was not to limit security effectiveness, those delegated the day to day security matters did not feel they were given adequate time to properly administer the security program. Applicant's supervisors felt he had transitioned well into the facility managerial role, and Applicant was given an overall performance rating of above average on November 15, 1991. On the advice of the DIS ISS assigned to company B, Applicant took part I of the Essentials of Industrial Security Management correspondence course[(4)] which he completed in March 1992. While he also enrolled in the second part of that course, he never completed it.

Applicant interacted with representatives of DIS when they performed security inspections of the facility as he would be briefed of the DIS findings. A medium sized facility within the Defense Industrial Security Program cleared to the Top Secret level on October 17, 1990, company B was authorized for storage of classified documents and hardware up to the Secret level. Approved for storage were a class B vault and a four drawer GSA approved container. Prior to 1992, all cleared employees of company B had access to the vault. During a DIS security inspection of the facility in early 1992, DIS cited as needing correction the lack of control to the vault. Consequently, the combination to the vault was changed in February 1992, and access limited to Applicant and co-workers C, D and E who were assigned primary or alternate security duties. A senior Tempest engineer (co-worker F) cleared to the Top Secret level with COMSEC access who had been with company B since September 25, 1967, recognized the change as a restriction on his ability to perform his job. On occasion, work was not completed as timely due to his inability to access the vault and obtain the classified material necessary to perform his work. At the request of co-worker F, Applicant had the four drawer classified storage container placed outside the vault to be used for the storage of classified material when in use by the cleared employees.

Co-worker F was well familiar with the requirements for handling and safeguarding classified information, to include COMSEC, having been provided by co-worker C with the required security briefing and COMSEC briefing statements.[(5)] Aware that a computer had to be approved by DIS before it could be used for the processing of classified information, co-worker F was found in February 1992 around the time of the vault combination change to be using his uncleared computer to process a classified report. Later that same day, another co-worker was discovered using his

unapproved computer system in similar fashion. Both were advised by co-worker C to stop the practice. On being notified, Applicant commenced the process to have both automated information systems (AIS) approved for classified work. DIS subsequently granted approval for both the systems.

Over the next few months, co-worker F gradually became lax in returning classified information to the vault. He began to leave classified information in his office desk and in a two drawer file cabinet adjacent to his desk. Co-worker F rationalized that the restricted area (considered by DIS to be a protected area) where his office was located provided the necessary protection for the classified information he required.[(6)] Approximately three times a week during a three week period in June 1992, co-worker D found classified working papers and documents sitting out on co-worker F's desk at lunchtime. Co-worker D notified Applicant twice about the incidents and requested that an inspection be conducted of co-worker F's desk in order to determine whether co-worker F was improperly using his desk for storage of classified information. An inspection of the desk was not conducted because Applicant did not consider it necessary.

Over the August/September 1992 time frame, co-worker G who was an engineer and program manager cleared Top Secret and COMSEC briefed, found internally generated classified material unsecured on co-worker F's desk on three separate occasions. Prior to the last incident which was on September 11, 1992, co-worker G, who had no official security responsibilities, asked co-worker D, the security administrator and alternate COMSEC custodian, to formally document the violation. Co-worker D advised co-worker G that it was Applicant's responsibility as FSO so co-worker G advised Applicant co-worker F had failed to properly secure classified information. Applicant talked to co-worker F about the situation but he otherwise took no action. On September 11, 1992, co-worker G was acting security monitor for the day. While doing a routine sweep of the building prior to closing and setting the building alarm, co-worker G found on co-worker F's desk an unmarked stack of papers containing Tempest test plans (TTP) and graphs with test data. Per the classification guidelines, the material was classified Secret. Co-worker G secured the material in the GSA approved security container and left a note for security administrators co-workers C and D that he found classified information out on co-worker F's desk for the third time in the last three months. The note was placed in co-worker F's personnel file but the security administrators took no further action as they felt it was Applicant's duty to do so as FSO. Although Applicant was aware that co-worker F left classified information unsecured on up to five occasions, he never took any formal disciplinary or reporting action as he did not consider the violations serious.

Starting in mid to late 1992, co-worker F began to use the non-removable hard drive ("fixed disk") of his office computer for the storage of classified information even though he knew the fixed disk was not approved for storage. In late 1992, it was discovered that one of the classified documents in co-worker F's possession had been taken apart and pages inserted into the document he was working on. All of the pages were reinserted into the original document. According to co-worker D, from that point on, all of the documents co-worker F used had to page counted. Also, about the same time, an unmarked disk was found among co-worker F's documents. In checking the disk, co-workers C and D noted that the disk contained a classified test report, and that in the directory read-out, the times were not during company B's working hours. Co-worker F's computer was checked to see if the time on the computer corresponded with the time on the disk. The security administrators' findings were inconclusive so no further action was taken.

Under time constraints and experiencing increasing difficulties in obtaining classified information from the vault when he needed it (those who had the combination were either out of the office or gone home for the day), co-worker F on April 27, 1992, in an effort to get the work done, removed computer disks and working papers classified up to the Secret level to his residence where he improperly used his home computer to process classified information. Co-worker F discovered that he could take raw data home and on his personal computer generate a "print file" for each table, graph or drawing in 15 to 20 seconds versus 10 to 15 minutes on the computers at work. On about eighteen occasions over the next two years to April 19, 1994, co-worker F removed classified information up to the Secret level on a floppy disk to his residence, usually overnight, although on three to four occasions, he took the material home for the weekend. The "print files" generated at home were stored on a disk and then returned to work where they could be copied to the printer in a continuous format. The disks used as storage for the print files were logged into the accountability system at work. Co-worker F processed the classified information at his residence in private. When not in active use, the classified was kept in his locked briefcase. In addition to processing classified information on his unapproved personal home computer, co-worker F, on at least two occasions between August 1993 and April 1994, printed classified information on his unapproved personal laser printer at his residence. Co-worker F was aware that the removal of the classified information to his residence was not authorized.

During a routine, scheduled inspection of the facility on September 2, 1993, DIS Industrial Security Specialist (ISS) H discovered two Secret files resident on the fixed disk of the AIS in co-worker F's office. Although the system was approved for classified processing, this was an unauthorized use of the hard drive. A letter of requirement was issued because of this improper storage and the fact co-worker F's system was connected to an unclassified local area network when he processed classified information. The company AIS Standard Practice and Procedure Manual (SPPM) was cited as deficient for failing to reflect proper disconnect procedures. ISS H rebriefed co-worker F regarding the proper procedures to declassify the hard drive to be followed when using the AIS for processing classified information. In Applicant's absence, co-worker G was briefed of the results of the inspection and instructed to revise the AIS SPPM to reflect it would not be a stand alone system and to include proper disconnect procedures. On return from temporary duty, Applicant was advised by co-worker G of the discrepancy on the disconnect procedures. Applicant left the correction to co-worker G and he never checked the AIS SPPM to see whether the document had been changed.[(7)]

Co-worker F gradually became lax about completing audit trail records[(8)] for the approved computer system in his office, executing no audit trail records whatsoever for the classified material which he generated on his office AIS subsequent to October 5, 1993.

On or about April 13, 1994, co-worker F removed nine classified computer disks and confidential specifications from the vault area which he used sometime over the next week in preparation of a Secret COMSEC TTP. He removed all the disks that might contain needed information because he was not certain on which disk(s) the information was stored. Most nights during the week he stored the disks and specifications in the GSA approved security container overnight as he did not want to keep running back to the vault. On or about April 19, 1994, he removed the disk on which he had been preparing the Secret COMSEC TTP to his residence, processed classified on his unapproved home computer and printed a revised TTP on his personal laser printer. On or about April 20, 1994, co-worker F gave the classified TTP (approximately 70 pages in length) to a cleared secretary at company B and asked her to add page numbers and figure titles. This secretary noted that the format in the report was not the same as she used when typing TTPs, but that it resembled the format used by co-worker F's spouse when she had worked at company B. The secretary asked co-worker F for the original classified disk on which the report had been generated. Co-worker F told her not to worry about it and to use the page numbering and figure title system from a similar report.

The secretary reviewed the audit trail log book for the approved computer systems and noted that the log did not reflect any classified processing activity since October 5, 1993, on any of the approved AIS. Suspecting that the document was not printed on the only laser printer which had been approved for classified processing, the secretary notified co-worker G. After his own review of the TTP, co-worker G suspected co-worker F had removed classified information to his residence and possibly co-worker F's spouse had assembled the TTP. Co-worker G immediately informed Applicant as well as co-worker C of his suspicions. At the recommendation of co-worker G, an internal investigation commenced. Co-worker C attempted to locate in the vault the disk on which the report was generated. In searching the disk file box in the vault area, co-worker G discovered nine Secret disks and one Confidential specification document were missing. Over the April 25 to 27, 1994 time frame, co-worker C conducted a complete audit of company B's classified holdings, which consisted of over four hundred classified items, fifty-seven of which were classified computer disks. Unable to locate the missing disks, co-worker C confronted co-worker F about his knowledge of the missing classified holdings. Co-worker F retrieved the nine Secret disks and Confidential specification from his desk and returned the items to co-worker C about 30 to 45 minutes later.

Co-worker G informed Applicant on April 27, 1994, that co-worker F had in fact removed classified material to his residence and processed classified on his unapproved home computer. Co-worker G informed Applicant he would call DIS and recommend impoundment of co-worker F's home computer. Applicant let co-worker G, who though cleared had no official security responsibilities, take the lead, and on the following day, co-worker G left a message for DIS ISS H who was on leave. On May 2, 1994, co-worker G informed DIS of the suspected mishandling of classified information by a cleared engineer of company B. An administrative inquiry (AI) was conducted by DIS, with Senior ISS I in charge, over May 3-6, 10-12, and 16, 1994.

During the first day of the AI on May 3, 1994, co-worker C found two Confidential classified documents lying out on the computer work table in co-worker F's office when co-worker F was out to lunch. ISS I was immediately notified,

and at her direction, the documents were secured. During a subsequent inspection of co-worker F's office, DIS discovered the several Confidential and Secret working papers on and in co-worker F's desk and in the two drawer file cabinet adjacent to his desk. Some of the classified documents were not marked with the appropriate classification level. The non-removable hard drive on the AIS in co-worker F's office was also checked with the assistance of co-worker C who retrieved the directory. Classified information was improperly stored on the fixed disk. Also, it was determined that some of the computer files had been generated off-hours and on weekends, at times when co-worker F was not at the facility. Following an interview of co-worker F in which he admitted to DIS that he had processed classified material at his residence, ISS I, a DIS Special Agent, a Government computer specialist and co-worker C accompanied co-worker F to his home on May 5, 1994, where a disk wipe was performed of his home computer.

Applicant was interviewed during the course of the AI. He acknowledged he was aware co-worker F had left classified material unprotected out on his desk approximately "a handful of times,"(9) but he did not know co-worker F was removing classified material to his home. Asked by DIS why an inquiry had not been conducted into co-worker F's suspected mishandling of classified information, Applicant responded he was not fully aware of the requirements pertaining to the procedures to be followed when violations of the Industrial Security Manual for Safeguarding Classified Information (ISM) occurred at the facility, to include the basics of conducting an inquiry. He stated that he did not think any compromise occurred because co-worker F's office was in the "secure area" of the engineering lab. Applicant indicated that he did not file an individual culpability report with DIS or take any individual administrative disciplinary action because he was not aware of the requirements. He denied any prior knowledge of co-worker F's improper storage of classified material in either his desk or two drawer file or that co-worker F had been taking classified material home since April 1992. Applicant admitted to DIS that the parent company took a "dim view" of any security violations.

DIS' findings following the AI were that since about April 1992, co-worker F had repeatedly and knowingly mishandled information classified up to the Secret-COMSEC level. On at least eighteen occasions over a two year time period (April 1992 to April 20, 1994) co-worker F removed classified information from the facility to his home, in violation of paragraph 5-106 of the ISM (DoD 5220.22-M). Co-worker F worked with the classified information at his home and he used his personal home computer to process classified information, to include making print files which were copied from a floppy disk taken from company B and generating a new floppy containing classified material. DIS also adjudged co-worker F culpable of printing classified at least twice on his laser printer at home, and improperly storing it in his briefcase at his residence when he was not working on it. His unauthorized processing and storage of the classified material was in violation of paragraphs 5-106, 8-100, 8-101, and 8-105 of the ISM. In the office, co-worker F was determined by DIS to have improperly stored in his desk and adjacent two drawer file cabinet classified material, usually Confidential and Secret working papers pertaining to TPPs and TTRs, but including for a few days in April 1994 Secret disks and a Confidential specification in his desk. On several occasions, co-worker F left classified documents on his desk unprotected when he went to lunch, and he stored classified files on the fixed disk of his office computer even though he knew the approval for the AIS did not extend to the storage of classified on the non-removable hard drive. His mishandling of classified at the office was deemed to be in violation of paragraphs 5-102, 5-300, 5-304, 5-306, 8-105, 8-308, 8-309, 8-314, and Section XI of the COMSEC supplement to the ISM. DIS also found that co-worker F properly failed to complete the audit trail records when processing classified on his approved AIS in violation of ISM paragraph 8-305.

For his part, Applicant was adjudged to have failed to fulfill his responsibility under paragraph 1-201 of the ISM to administer the Defense Industrial Security Program at company B. Specifically, when apprised of security violations involving the classified material left unprotected on co-worker F's desk, he failed to conduct any inquiry into the reported violations, did not submit an individual culpability report on co-worker F to the Defense Industrial Security Clearance Office (DISCO), failed to rebrief co-worker F after learning of the violations, and did not take any disciplinary action against co-worker F. His failure to take the appropriate action was in violation of paragraphs 1-304, 1-305, 3-102, 3-105, and 1-211 of the ISM.

With respect to security education of cleared employees at company B, the company SPPM outlined the procedures to be followed when safeguarding classified information, and all employees had been given copies of the SPPM. Those who had access to an AIS approved for classified processing had company B's AIS SPPM available to them. DIS assessed the security education program as deficient in that there was no formal security education program in effect.

Although all personnel had their initial security briefings, the employees could not recall their last briefing and there was no recordation of rebriefings.(10) COMSEC briefings had been given on a yearly basis, and those were recorded.

On the issue of compromise, access to co-worker F's office area was assessed as "somewhat" controlled, in that all personnel in the area possessed at least a Secret clearance, access was through cipher lock doors, all visitors were escorted, personnel had been given a COMSEC briefing, there was no indication of access by an unauthorized person, where classified had been found out in the open it was immediately retrieved and secured either in the vault or security container. Nonetheless, DIS determined that the probability of compromise of classified information could not be precluded due primarily to co-worker F having taken classified material home.

Due to the security problems discovered during the AI, an unannounced inspection of the facility was conducted by DIS on May 11 and 17, 1994. During the inspection, DIS found that the company had failed to correct a deficiency discovered during the September 2, 1993 prior routine inspection in that the AIS SPPM had not been updated to reflect proper disconnect procedures when processing classified information. The overall security posture of the facility was assessed as unsatisfactory(11) as the overall results of the inspection and AI revealed that security management could not be depended on to initiate inquiries into reported security violations. Cited as major systemic deficiencies were Applicant's failure to ensure proper safeguarding of classified information; the lack of any system to discipline employees deemed culpable for security violations; the absence of any formal security education program to ensure periodic rebriefing of cleared employees; classified files had been found on co-worker F's fixed disk; and audit trail records had not been completed to reflect classified processing which had taken place in the facility over the January to April 1994 time frame. During the exit briefing, Applicant was advised of the unsatisfactory rating, and he was instructed to become more personally involved in the security program, to include developing procedures to report violations and discipline culpable employees, to outline a system of rebriefing and to remind AIS users of their responsibilities.

By separate letters dated June 9, 1994, Applicant as ---------- of company B and the President of the division's parent company were notified formally of the unsatisfactory rating assigned the facility due to co-worker F's serious security violations and Applicant's failure to fulfill his FSO responsibilities to ensure classified information was safeguarded properly and to provide management support needed to maintain an effective industrial security program. The user agencies were notified on that date of the unsatisfactory rating as well. Applicant was involuntarily terminated from his employment with company B on June 29, 1994, due to the security problems at the facility. He appealed the termination on July 27, 1994, but his firing was deemed appropriate due to the seriousness of the violations and Applicant being personally accountable for security at the facility.

Applicant was out of work for ten months following his termination. During his initial interview with his current employer (company A), Applicant mentioned that there had been a security related issue associated with his departure from company B, although he was not completely forthcoming about the details. The group vice president called co-worker G with whom he was acquainted to get a better understanding of the circumstances involved in Applicant leaving the employ of company B. Co-worker G did not consider it appropriate to go into any detail but stated that the incident involved another employee and that Applicant as FSO had been compelled to accept responsibility for inadequate reporting. Applicant was hired by company A and placed on unclassified tasks. With the subsequent revalidation of his security clearance at the Secret level, Applicant was given classified duties in the AIS area where he performs ----------. In that capacity, he works closely with security regulations. Applicant has proven to be an excellent and reliable -------- for company A.

POLICIES

The adjudication process is based on the whole person concept. All available, reliable information about the person, past and present, is to be taken into account in reaching a decision as to whether a person is an acceptable security risk. Enclosure 2 to the Directive sets forth adjudicative guidelines which must be carefully considered according to the pertinent criterion in making the overall common sense determination required. Each adjudicative decision must also include an assessment of the seriousness, recency, frequency and motivation for an applicant's conduct; the extent to which the conduct was negligent, willful, voluntary, or undertaken with knowledge of the circumstances or consequences involved; the age of the applicant; the absence or presence of rehabilitation, the potential for coercion or

duress, and the probability that the conduct will or will not recur in the future. *See* Directive 5220.6, Section F.3. and Enclosure 2. Because each security case presents its own unique facts and circumstances, it should not be assumed that the factors exhaust the realm of human experience or that the factors apply equally in every case. Moreover, although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility or emotionally unstable behavior.

Considering the evidence as a whole, this Administrative Judge finds the following adjudicative guidelines to be most pertinent to this case:

SECURITY VIOLATIONS

Noncompliance with security regulations raises doubts about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Conditions that could raise a security concern and may be disqualifying include:

(2) violations that are deliberate or multiple or due to negligence.

Conditions that could mitigate security concerns include actions that:

None.

* * *

Under the provisions of Executive Order 10865 and the Directive, a decision to grant or continue an applicant's clearance may be made only upon an affirmative finding that to do so is clearly consistent with the national interest. In reaching the fair and impartial overall common sense determination required, the Administrative Judge can only draw those inferences and conclusions which have a reasonable and logical basis in the evidence of record. In addition, as the trier of fact, the Administrative Judge must make critical judgments as to the credibility of witnesses. Decisions under the Directive include consideration of the potential as well as the actual risk that an applicant may deliberately or inadvertently fail to properly safeguard classified information.

Burden of Proof

Initially, the Government has the burden of proving any controverted fact(s) alleged in the Statement of Reasons. If the Government meets its burden and establishes conduct cognizable as a security concern under the Directive, the burden of persuasion then shifts to the applicant to present evidence in refutation, extenuation or mitigation sufficient to demonstrate that, despite the existence of criterion conduct, it is clearly consistent with the national interest to grant or continue his security clearance.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. Where the facts proven by the Government raise doubts about an applicant's judgment, reliability or trustworthiness, the applicant has a heavy burden of persuasion to demonstrate that he is nonetheless security worthy. As noted by the United States Supreme Court in *Department of Navy v. Egan*, 484 U.S. 518, 531 (1988), "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials." As this Administrative Judge understands the Court's rationale, doubts are to be resolved against the Applicant.

CONCLUSIONS

Having considered the evidence of record in light of the appropriate legal precepts and factors, and having assessed the credibility and demeanor of those who testified, this Judge concludes that the Government has established its case with regard to Criterion K.

The Government has an unequivocal need to protect classified information within the defense industry. Therefore, security clearances will be awarded only those applicants who demonstrate the appropriate good judgment and reliability in the protection of such information. The evidence establishes that co-worker F over the April 1992 to May 4, 1994 time frame knowingly and willfully disregarded the procedures for the safeguarding of classified material set forth in the Industrial Security Manual for the Safeguarding of Classified Information (DoD 5220.22-M),[(12)] to wit: he on about eighteen occasions removed material classified up to the level of Secret-COMSEC to his residence; processed classified information on his personal computer which was not approved for such processing; twice printed classified on his home laser printer; stored classified material in his briefcase at his residence; repeatedly stored classified material on his fixed hard drive at work, in his office desk and in a two-drawer file cabinet adjacent to the desk; failed to maintain any audit trail records for processing of classified performed after October 5, 1993; and on several occasions between at least June 1992 and May 4, 1994, left classified information out in the open in his office when he went to lunch. Applicant bears significant responsibility for the violations of this employee, not only by virtue of his position as ----------, but also because of his failure to take appropriate action when apprised of specific violations.

Under ¶1-201 of the ISM, the senior management official at a facility cleared within the Defense Industrial Security Program has the primary, undelegable responsibility to ensure that the classified material entrusted to the facility is adequately safeguarded. When he accepted the position of ---------- in October 1990, Applicant also assumed the official duties of facility security officer. Applicant took a "hands-off" approach to security, leaving the program essentially as it had been prior to his tenure as FSO. Day to day implementation of the security program was left to other cleared employees, primarily co-workers C and D (and after December 13, 1993, to C and E). While he could delegate security functions to other cleared and appropriately trained personnel, he was required to supervise and direct security measures necessary for the proper application of U.S. Government furnished guidance or specifications for classification, downgrading, upgrading, and for safeguarding classified information. *See* ISM ¶1-201. On being apprised that co-worker F had processed classified material on his unapproved office computer, Applicant followed through with gaining approval from DIS for co-worker F's computer. At the request of co-worker F, Applicant also directed that the GSA approved security container be removed from the vault to facilitate employee access when working on classified material. For the most part, however, he failed to direct appropriate security measures, electing instead to devote his attention to the business needs of the facility. Under pressure to keep overhead costs to a minimum, Applicant attempted to budget security, which had the adverse, albeit unintended, consequence of undermining the security program. Those tasked with the day to day implementation of security were not afforded sufficient time to properly manage the program.

That business interests predominated is most evident in Applicant's failure to take appropriate action when apprised of co-worker F's security responsibilities. In June 1992, Applicant was apprised twice by co-worker D that co-worker F was leaving classified material[(13)] out on his desk at lunchtime. Applicant refused co-worker D's request to conduct a search of co-worker F's desk because he did not think it was necessary. His failure to initiate a preliminary inquiry to ascertain whether there was a compromise is a violation of ¶ 1-304 of the ISM as well as ¶ 3.3 of company B's SPPM.[(14)] It was not until sometime in the August/September 1992 time frame, when Applicant was informed by co-worker G that co-worker F had again been caught leaving classified material unprotected out on his desk, that Applicant took any action whatsoever, and this was limited to talking to co-worker F. Applicant failed to comply with the mandatory reporting requirements set forth in ¶¶ 1-304 and 1-305 of the ISM. Applicant was not aware at that time that co-worker F on at least one occasion in April 1992 had deliberately disregarded both the ISM and company SPPM provisions prohibiting removal of classified material to his residence,[(15)] but he knew Applicant had left classified material unprotected in June 1992 so this was a repeat violation. Under ¶ 1-305, an individual culpability report must be submitted to DISCO when there is a pattern of negligence or carelessness, defined as two or more violations in a 12-month period. Pursuant to ¶ 1-211 of the ISM and ¶ 3.5 of the SPPM, a final report is to be filed which identifies the culpable individual and includes a statement of corrective action taken.

As noted, the only corrective action taken was to speak with co-worker F sometime prior to September 11, 1992. Since co-worker G found a Secret TEMPEST document unprotected in co-worker F's office on September 11, 1992, the remedial action taken by Applicant was obviously insufficient. He failed to ensure that co-worker F was rebriefed with respect to his security responsibilities or to take any disciplinary action. Pursuant to ¶ 1-211 of the ISM, contractors are to establish and enforce policies that provide for appropriate administrative actions against employees who commit security violations and that a graduated scale of disciplinary actions is to be applied. On review of the company SPPM

during the course of the AI, it was discovered that the SPPM did not contain any such graduated disciplinary sanctions. It cannot be determined with any certainty if co-worker F's subsequent violations (to include the very serious removal of Secret-COMSEC material to his residence and processing it on his unapproved home computer) would have been prevented if Applicant had complied with mandatory reporting or disciplinary requirements. Applicant admits he did not report the violations in part because he did not want to jeopardize co-worker F's employment as the parent company had a "dim view" of security violations.(16) What is clear is that Applicant put the interests of co-worker F and company B above his obligation to ensure that classified material entrusted to the facility was appropriately safeguarded.

During the unannounced inspection of the facility in May 1994, classified material was found resident on the non-removable hard drive of co-worker F's office computer. While this was a knowing violation of ISM ¶ 8-311 committed by co-worker F, Applicant must be held accountable for failure to appropriately document disconnect procedures in company B's AIS SPPM after being advised by DIS of the deficiency during a prior inspection in September 1993. The evidence reflects that Applicant was on TDY at the time of the September 1993 inspection and that co-worker G received the exit briefing from DIS. Applicant claims he left the correction to co-worker G, who it is noted had no official security responsibilities apart from his obligation as a cleared, COMSEC briefed employee to adhere to the requirements of the ISM and company SPPM. Indicative of his reactive approach to security, Applicant made no effort to ensure that the deficiency was corrected.

He also failed to periodically review or at least have his COMSEC custodian or security manager review the audit trail logs associated with classified work processed on co-worker F's office computer. Pursuant to ¶ 8-305 of the ISM, audit trails are to be reviewed and annotated at least weekly to ensure that all pertinent activity is properly recorded and appropriate action taken to correct anomalies. Had the audit logs been reviewed as required, the company may have discovered prior to April 20, 1994, that co-worker F had been improperly removing classified material from the facility and thereby subjecting it to possible compromise.

DIS also cited as deficient security education at the facility and the procedures to identify AIS storage media. Although the facility was not in strict compliance with ISM requirements in regard to both education and AIS markings, there was not a complete system failure. Under ¶ 3-104 of the ISM, the contractor is to inform employees of their responsibility for the safeguarding and handling of classified information, of the security requirements particular to their job assignments and a counterintelligence awareness briefing. Employees at company B were apprised on a yearly basis of their COMSEC responsibilities, but there was no evidence of general refresher briefings which are required in ¶ 3-105 of the ISM. (17) Co-worker F, who committed the security violations which led to the AI, stated that he had been briefed on a yearly basis and he was aware of his security responsibilities. The DIS assessment is based primarily on the absence of recordation and the fact that all cleared employees could not recall the date of their last general security briefing. ISS I found that all cleared employees had their initial briefings and had executed classified information non-disclosure agreements. With respect to the AIS media, ¶ 5-206 c. of the ISM provides that Top Secret and Secret storage media shall be entered into accountability as soon as classified information is recorded on the media. Confidential need not be entered into accountability, but there must be a general description of the classified information contained on the storage media. DIS found that the 57 Secret diskettes and 9 Confidential diskettes in company B's possession had been entered into accountability, although with not enough identifying information.

By virtue of his position as ---------- and FSO, Applicant had an affirmative obligation to ensure compliance with the ISM. Where he himself breached the requirements, he bears a particularly heavy burden to demonstrate it is clearly consistent with the national interest that he retain his security clearance. In assessing the current security significance of his failure to maintain adequate security at company B, this Administrative Judge must take into account the Adjudicative Guidelines pertaining to security violations. There is no evidence that there was any unauthorized disclosure of classified information. Disqualifying condition (DC) 2 is however pertinent. Applicant committed multiple violations of the ISM when he failed to investigate reports of classified information being left unprotected by co-worker F, failed to file mandatory reports of the repeated violations committed by co-worker F, and failed to discipline or impose an administrative sanction on co-worker F. When asked during the AI why no inquiry was conducted surrounding the violation, Applicant replied that he was not fully aware of the requirements to be followed when violations of the ISM occurred at the facility and that he did not think any compromise occurred because co-worker F's office was within the "secure area." He also indicated he was not aware of the requirement of filing an individual culpability report or taking administrative disciplinary action. Interviewed on November 6, 1995, Applicant reiterated

that he did not consider it a serious violation, and that while it was poor judgment on his part, he did not knowingly disregard his security responsibilities. In his Answer, Applicant provided three reasons for his failure to report co-worker F, to wit: co-worker F was a long time employee and Applicant did not want to jeopardize co-worker F's position within the company and his retirement; the risk of compromise was extremely minimal; and co-worker F had been prior to 1980 security administrator at the facility and should have been cognizant of the rules anyway. After considering Applicant's admission that the parent company took a dim view of security violations, it becomes clear that his failure to investigate, report or discipline co-worker F was intentional rather than from any lack of knowledge as to security requirements. In contrast, Applicant acted negligently in failing to ensure that company B's SPPM and AIS SPPM were appropriately updated to conform to the ISM.

The Administrative Guidelines provide for mitigation where the violations were inadvertent (MC 1), isolated or infrequent (MC 2), due to improper or inadequate training (MC 3), or demonstrate a positive attitude towards discharge of security responsibilities (MC 4). None of the corresponding mitigating conditions apply to Applicant's deliberate disregard of his security responsibilities to investigate, report and discipline an employee found culpable of repeated violations of the ISM and company SPPM. Applicant testified he received no formal briefing from anybody about the FSO responsibilities. (Transcript p. 143). DIS ISS H, to whom company B has been assigned since roughly 1982, admitted that when Applicant became FSO the emphasis would not have been as strong as for somebody off the street who had not been familiar with the Defense Industrial Security Program. (Transcript p. 206). To his recollection, he recommended to Applicant that he take the correspondence courses (Transcript p. 200). ISS H testified further that an FSO who had taken the Essentials of Industrial Security Management correspondence course would have a basic knowledge of how to administer a security program, which would include the processing of clearance requests, the education and training of personnel, and reporting requirements. (Transcript p. 209). Applicant completed that course in arch 1992, but recalled no specifics of the correspondence course at the hearing. Whereas Applicant had taken the correspondence course, had an ISM available to him for reference and had ISS H to contact if he had any questions, he had the knowledge and/or means to acquire that information needed to adequately manage the facility security program. Applicant also maintains in mitigation that when apprised of the very serious removal of classified material from the facility, he acted appropriately. Applicant did not take the lead in investigating or reporting the violation, but instead left it up to co-worker G, who although cleared and COMSEC briefed, had no official security responsibilities. Applicant did not violate any security requirement by delegating the duty, but his conduct even on that occasion was typical of his "hands-off" approach to security. Despite Applicant's retrospective acknowledgment that he should have reported co-worker F, concerns persist about whether Applicant appreciates the degree to which he failed as FSO. Those employees delegated the day to day operation of the facility were not given sufficient time by Applicant to fulfill their duties. Applicant has shown no understanding that his failure to reprimand co-worker F reflects a lack of management support for the security program.

The other violations cited in the SOR are due to Applicant's neglect of his FSO duties. With respect to Applicant's failure to incorporate disciplinary sanctions and AIS disconnect procedures in the SPPM and AIS SPPM, respectively, DIS discovered during an inspection of the facility in September 1993 that co-worker F had processed classified on his office computer when it was connected to a local area network, a serious violation. Proposed correction included updating the AIS SPPM to reflect proper disconnect procedures, which was not accomplished by May 1994. Applicant was grossly negligent in failing to bring his facility back into compliance with the Defense Industrial Security Program requirements. ISS H testified that during his September 1993 inspection, he found one administrative violation, but it involved retention of material. (Transcript p. 202). Applicant claims that had he been informed of the need to incorporate graduated disciplinary actions in the SPPM during previous inspections, the document would have been corrected. On review of an industrial security inspection report (Govt. Exhibit 7 p. 35), it is noted that the standard practice procedures is a specific element inspected by DIS both during announced and unannounced visits. There is no evidence that the facility was cited in September 1993 for the absence of graduated disciplinary actions from the SPPM. This does not absolve Applicant of his affirmative duty to ensure the company Standard Practice and Procedures were in compliance with the ISM. There is no evidence that he ever took it upon himself to determine whether the SPPM was updated or that the facility's practices, to include the accountability and markings of AIS storage media, were in compliance with current security regulations. To the contrary, Applicant admits that with the exception of a change to AIS configuration, the manuals remained as they had been prior to his assumption of the FSO position. In similar fashion, Applicant submits that security education was conducted as it had been in the past prior to his tenure as FSO. For obvious reasons, the Government cannot be present at each facility to oversee security operations, but must rely on

those cleared within the industrial security program to **affirmatively** fulfill their contractual obligations. The delegation of security functions to other cleared employees does not absolve him of his own negligence in failing to ensure that security practices were in compliance.

Since commencing his employ with company A in May 1995, Applicant has proven to be a productive and dependable worker. On reinstatement of his Secret security clearance, Applicant was given access to classified information, and there is no evidence that he has violated any security regulations. On balance, this favorable evidence is not sufficient to overcome the very serious concerns engendered by the aforesaid criterion K conduct. Accordingly, subparagraphs 1.a.(1), 1.a.(2)(a), 1.a.(2)(b), 1.a.(3), 1.a.(4), 1.a.(5) and 1.a.(6) are resolved against him.

FORMAL FINDINGS

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

Paragraph 1. Criterion K: AGAINST THE APPLICANT

Subparagraph 1.a.(1): Against the Applicant

Subparagraph 1.a.(2)(a): Against the Applicant

Subparagraph 1.a.(2)(b): Against the Applicant

Subparagraph 1.a.(3): Against the Applicant

Subparagraph 1.a.(4): Against the Applicant

Subparagraph 1.a.(5): Against the Applicant

Subparagraph 1.a.(6): Against 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.

Elizabeth M. Matchinski

Administrative Judge

1. On completion of Tempest testing of communications security equipment and components, cleared engineering personnel prepared Tempest Test Plans (TTPs) and Tempest Test Reports (TTRs) which were then submitted to the appropriate user agency for review. When preparing TTPs and TTRs cleared engineering personnel and laboratory technicians had access to classified reference documents. Classified information was extracted from these documents and incorporated into the TTPs and TTRs.

2. At his hearing, Applicant testified he did not receive any formal briefing from anyone about what the responsibilities of the FSO were (Transcript pp. 143, 175). However, in a signed, sworn statement dated November 6, 1995 (Government Exhibit 2), he indicated, "I became the Facility Security Officer (FSO) at [company B] in October 1990. I was briefed by the DIS Industrial Security Representative concerning my duties/responsibilities of a FSO."

3. According to Applicant, he accepted the FSO role because his predecessor did not appear to have much direct involvement in security functions (Transcript p. 142), and he conducted the security program in essentially the same manner as it had been since his employ in 1980. He testified that company B did not have any yearly security briefings or security awareness training during the period 1980 to 1990 and he continued that because he did not know any better. (Transcript p. 151).

4. The DIS ISS assigned to company B since about 1982 testified that an FSO who had completed the course would have a basic knowledge of how to administer a security program. (Transcript p. 209). According to ISS I, who conducted an AI at the facility in May 1994, the program covers the basics for all facilities involved in the Defense Industrial Security Program, including the various responsibilities for protecting classified information, the processing of individuals for clearance, the need to report adverse information and changes in ownership or conditions, conducting inquiries into suspected security violations, filing individual culpability reports, security education and rebriefings. (Transcript pp. 107-09). Applicant at the hearing could not recall the specifics of the correspondence course. (Transcript p. 175).

5. During an interview of May 10, 1994, in conjunction with an administrative inquiry conducted by DIS, co-worker F indicated he was given COMSEC refresher briefings on a yearly basis which consisted of co-worker C having him read and signing the briefing statements. (Government exhibit 7).

6. The evidence reflects that all employees at company B possessed at a minimum a Secret security clearance, all visitors were escorted, and the building was equipped with an alarm system.

7. Applicant testified he was told the problem had been taken care of. He did not personally check the AIS SPPM to see whether the disconnect procedures had been incorporated as he did not understand it to be a serious problem. (Transcript pp. 185-86).

8. As testified to by DIS ISS I, who conducted an administrative inquiry at the facility in May 1994, audit trails capture the usage of a particular accredited system for processing classified information (date, start and stop time, brief description of the information processed, user and identification of any printed or disk copies made). (Transcript p. 61).

9. Applicant testified that he did not report co-worker F because there was a minimal risk of compromise, i.e., it was a stand alone facility, all employees were cleared, visitors were minimal, cleaning and maintenance were performed by a cleared employee, the facility was alarmed at night, and there were cipher locks on all entrances. He also admitted that he did not want to jeopardize co-worker F's position in the company as he was a long-time employee close to retirement and the parent company had a dim view of security violations. (Transcript pp. 146-47). On cross-examination, Applicant admitted that he was aware that co-worker F's leaving classified information out on his desk in the open was a violation as the area was not approved for open-shelf storage, however. (Transcript p. 182).

10. During the AI, DIS traced the briefings back to 1991. (Transcript p. 125).

11. Applicant claims he was told the facility was going to get a conditional rating, (Transcript p. 155), and that he was in shock when he received the June 9, 1994 letter apprising him of the unsatisfactory rating. (Answer to SOR). ISS I testified that she told Applicant the facility would be rated unsatisfactory. (Transcript p. 127).

12. All references to the ISM herein are to the version of DoD 5220.22-M dated January 3, 1991.

13. Pursuant to ¶ 1-304 of the ISM, each security violation involving COMSEC information, irrespective of compromise or suspected compromise, must be reported to the cognizant security office. Co-worker F admitted that the working papers which he left out on his desk in 1992 pertained to a certain TEMPEST test contract. Under the terms of that contract, access to accountable COMSEC material was required.

14. Pursuant to ¶ 1-304.a. of the ISM, "[i]mmediately on receipt of a report of loss, compromise, or suspected compromise of classified information, the contractor (FSO) shall initiate a preliminary inquiry to ascertain all of the circumstances surrounding the reported loss, compromise, or suspected compromise, or security violation." The company SPPM specifically provides under ¶ 3.3 that it is the FSO's responsibility to initiate the preliminary inquiry.

15. It is not at all clear to this Administrative Judge that co-worker F inadvertently left the classified material unprotected when he went to lunch, given his demonstrated disregard for the prohibition against removal of classified to his residence.

16. During the AI, co-worker G indicated to DIS that company policy mandated that co-worker F should have been fired

for the first or second offense.

17. Pursuant to ¶ 3-105, "[p]eriodically contractors shall rebrief all cleared employees to (i) remind them of their continuing responsibilities for safeguarding classified information; (ii) ensure they are aware of the security procedures pertaining to their particular work assignment; (iii) ensure they are aware of any security deficiencies resulting from inspections that require their individual attention to bring about corrective action; (iv) indoctrinate them in the methods and operations used by [hostile intelligence services] to subvert U.S. industrial personnel; and (v) defensive measures to counter such subversion attempts."