DATE: July 23, 1997

In re:

SSN:

Applicant for Security Clearance

ISCR OSD Case No. 96-0605

DECISION OF ADMINISTRATIVE JUDGE

ELIZABETH M. MATCHINSKI

APPEARANCES

FOR THE GOVERNMENT

Barry M. Sax, Esq.

Matthew E. Malone, Esq..

Department Counsel

FOR THE APPLICANT

Arthur S. Keyser, Esq.

Mary Vassallo Slinkard, Esq

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) pursuant to Executive Order 10865 (as amended by Executive Orders 10909, 11382 and 12829) and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992 (as amended by Change 3) issued a Statement of Reasons (SOR) dated November 4, 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 December 12, 1996, Applicant responded to the allegations set forth in the SOR and requested a hearing. The case, originally assigned to Administrative Judge Paul J. Mason, was transferred to the undersigned due to workload considerations on January 15, 1997. Accordingly, on January 16, 1997, the undersigned scheduled the hearing for February 14, 1997. The parties stipulated to the admission and pre-hearing consideration of sixteen Government exhibits. Two Applicant exhibits were also submitted into the record before the hearing, the Government having no objection to their admission.[(1)]

At the hearing held as scheduled on February 14, 1997, testimony was taken from five witnesses: a Defense Investigative Service Industrial Security Specialist (DIS ISS), an Assistant Facility Security Officer (Asst. FSO) at

Applicant's employment, a co-worker of Applicant's (co-worker B), Applicant's direct supervisor, and the Applicant. At the motion of the Government, the Statement of Reasons was amended at the hearing, adding a second paragraph alleging violation of criterion E, personal conduct, as follows:[(2)]

2. Criterion E: Personal conduct, conduct involving questionable judgment, untrustworthiness, unreliability or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. Available information raising this concern shows that:

a. On April 24, 1996, Applicant deliberately provided false or misleading information concerning relevant and material matters to an investigator of the Defense Investigative Service, [Special Agent C], in connection with a personal security or trustworthiness determination, to wit: that he, Applicant, punched a hole in the floppy disk as is alleged in allegation 1.e., above, in March of 1996, when in truth and in fact, as [Applicant] has now admitted, it was [co-worker B] who actually punched the hole in the floppy disk.

Also, during the course of that proceeding, the undersigned ordered the Government to provide to Applicant's counsel after the hearing a sanitized copy of the classified notes, which were found in Applicant's desk on February 5, 1996, and which are the subject of subparagraphs 1.a. and 1.b. of the SOR. The parties were advised that this Administrative Judge would entertain a request to reopen the hearing following counsel's review of the sanitized notes. Over the Government's objections, the undersigned on March 10, 1997, granted Applicant's request to reopen the record to question witnesses and present new evidence relevant and material to the matter at issue. Pursuant to an amended notice, the hearing was reconvened on April 4, 1997, during which testimony was taken from a chief scientist at Applicant's employment, as well as from the Asst. FSO, co-worker B and Applicant. Two additional Applicant exhibits were admitted into the record. Department Counsel withdrew allegation 1.e. of the Statement of Reasons.[(3)] A transcript of the April 4, 1997, proceeding was received in this office on April 15, 1997. On May 15, 1997, Applicant's counsel timely filed written closing argument. With the receipt of Department Counsel's rebuttal argument dated May 30, 1997, the case was ripe for a decision.

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 38 year old ---------- employed as a ---------- of the ---------- staff at a defense contractor ---------- (company A). Applicant has worked for this same organization[(4)] since May 28, 1985. He seeks to retain a Secret security clearance which was granted to him on July 24, 1985, for his work on classified radar projects there.

Circa 1988, Applicant obtained unclassified handwritten notes[(5)] from a co-worker pertaining to an engineering calculation formula used to determine various radar power density values specific to Government contracts on which Applicant was working for his employer. In 1989, Applicant began adding to the notes in his handwriting formulas and calculations until the document reached some thirty-two pages in length.[(6)] To this document, Applicant knowingly entered frequency range, power levels and/or instantaneous bandwidth information pertaining to at least two different radar systems which was classified Confidential per the particular contracts between company A and the Government User Agency. App. Exh. A p. 19. In addition, on two pages he added Confidential information pertaining to an electronic warfare program.[(7)] Some of the information entered, such as the specific frequency at which a certain radar system operated, was classified in and of itself. Some of the information was classified because it was entered in a formula or calculation in such a manner that it could be associated with a particular radar system. The classified information entered was rather basic to Applicant's work.[(8)]

Applicant does not dispute that classified information was entered into the document, although he submits it was limited to two, at most three, sets of numbers (Govt. Exh. 2; Tr. 2/14/97 p. 117-18, 138; Tr. 4/4/97 pp. 96-97). On direct examination during the first hearing, he indicated classified information was limited to two pages, one which got inadvertently clipped in. Tr. 2/14/97 p. 138. Applicant's position is that the radar frequency information relating to one particular radar system (radar set #1), which he submits was found on the first and second pages of the thirty-two page

document and determined by the chief scientist to be classified, was neither classified nor present with other information which was classified. *See* Tr. 2/14/97 p. 120; Tr. 4/4/97, p. 96. In support of his contention, he points to a published table in an unclassified text (App. Exh. B) which lists the transmitter type, frequency range (in MHz) and operating bandwidth (in MHz) for the radar set which is identified by name. The chief scientist, who had the opportunity to review the working papers against the security classification guidance for general radar (*See* Tr. 4/4/97 pp. 86-87), testified as follows:

I would be suspicious of three numbers on that first page. The frequency band at which the emitter is able to transmit and receive is unclassified. The specific frequency at which it is able to transmit and receive is still classified. So it would be one number that would be classified since the frequency is given in megahertz. The guideline clearly delineates the specific frequency at which the radar operates to be classified. The other two numbers that I would anticipate being classified would be peak power and instantaneous bandwidth.

Tr. 4/4/97 pp. 45-46. The chief scientist testified he was not familiar with the number listed under frequency range in the table claimed by Applicant to be unclassified. Tr. 4/4/97 p. 39. However, he makes a valid point that the fact that something appears in the public domain does not render it unclassified. If the Government agency guidelines indicate by contract specification that the information is to be considered classified, then the defense contractor (here company A) must treat it as classified.[(9)] It is noted that co-worker B, who possesses a working familiarity with the classified radar information at issue, no longer views as classified one output power value pertaining to radar set #1 which was in the notes and identified by the chief scientist as Confidential:

There was one value given for the power--output power for the [radar set #1] which was crossed off as being classified. Based on other documentation that we have that would indicate that the value is in fact not classified. At the time a certain document that [Asst. FSO] produced indicated that by certain guidelines it would be considered Confidential whereas by other guidelines as she indicated different guidelines are applicable to different contracts. So that item was suspected as not being classified and in the course of the discussion it was determined that in other documentation at least by different agencies it had been treated unclassified. By documents released by our own company it was treated as unclassified. And I think the understanding was, that was a result of treaty agreements between the Soviet Union that the information had to be divulged anyway which is my current understanding.

Tr. 4/4/97 p. 101-02. Notwithstanding the expert qualifications of the chief scientist gained by working with radar since 1959 (Tr. 4/4/97 p. 59), there is insufficient evidence to determine whether or not the power output number pertaining to radar set #1 is classified. The chief scientist testified that on his most recent review, he referred to the "security guideline provided which was attested to be the one under which would have been applied to the generation of this particular book at the time." Tr. 4/4/97 pp. 58-59. Whereas he was not familiar with the number at issue, it was especially important that the chief scientist be provided the contract specific classification guideline. According to the chief scientist, what is classified from time to time depends on the classification guideline which applies to the contract under which one is operating. Tr. 4/4/97, pp. 59-60. The security classification guideline reviewed was provided to the chief scientist by company A's security department. Tr. 4/4/97 p. 59. The Asst. FSO testified that the chief scientist used a "classification guidance for *general radar* that was applicable at the time frame the document was originally written." Tr. 4/4/97 p. 88 (emphasis added). It is unclear whether the power output value was to be treated as classified under the contract(s) Applicant was working on. Thus, no definitive factual finding can be made as to the nature (classified or not) of the power output value.[(10)]

The chief scientist determined there were at least two other numbers on the first page of the notes which were classified Confidential, however. *See* Tr. 4/4/97 pp. 45-46. Applicant failed to mount a successful challenge to that testimony.[(11)]

Co-worker B, who also works with the classified information at issue, on cursory review of the notes when he found them on February 5, 1996, determined three of the pages contained classified frequency ranges listed directly below the name of the corresponding radar system. *See* Govt. Exh. 9. After the chief scientist reviewed the document for purposes of sanitizing it, co-worker B had an opportunity to see it again. Co-worker B identified at least one more item as Confidential which had not been marked as classified by the chief scientist on his reviews. This Administrative Judge finds it significant that co-worker B, who has a working familiarity with the radar projects at issue in this case, does not dispute the classification assessment rendered by the chief scientist, with the lone exception of the one power output

value. The extent to which classified Confidential information is contained in the working papers cannot be determined precisely, as the power output value may well not be classified, but there is sufficient information in the record, based on the classification assessment performed by the chief scientist and co-worker B's testimony to find Applicant knowingly inserted Confidential information on multiple pages.[(12)]

Applicant intentionally did not mark the document as classified.[(13)] Over the course of the next seven years (from 1989 to February 5, 1996), he referred to the document approximately three times per week in his work. When not using the notes, Applicant retained them in his unlocked desk drawer. (Govt. Exh. 2). During that period, Applicant shared a cubicle with co-worker B who also has a Secret clearance. Their cubicle was located in an open, non-secured area to which uncleared employees would have had access during the day and security and cleaning personnel at night. About three feet from his desk, Applicant had a four drawer container with a combination lock which was approved for the storage of classified information. Tr. 2/14/97 pp. 41, 48-49, 191. In 1995, Applicant was custodian of the classified storage container. *See* Govt. Exh. 2. Applicant did not secure the classified document in the approved storage container. Applicant did not believe that anyone could determine that the document was classified since the Confidential numbers were buried in formulas and the document did not bear any classification markings. Tr. 2/14/97 pp. 140-41, 154, 156; Govt. Exh. 2.

In approximately summer 1995, Applicant was asked to include in a document a table with Confidential radar range information. After typing the unclassified portion, Applicant went to a computer approved for the processing of classified information. Unable to get the word processing feature to work and in a hurry, Applicant took the floppy diskette out the computer approved for classified and completed the table on an unapproved computer located in the next cubicle with the intention of saving the information to the floppy. Govt. Exh. 2; Tr. 2/14/97 pp. 42, 112-13, 145-46. Co-worker B noticed Applicant entering the Confidential frequency band information and inquired as to his rationale for entering classified on an unapproved automated information system. Applicant explained to co-worker B that the word processor on the classified machine was not available and that he did not think there would be a problem because he was saving only on the floppy. Co-worker B advised Applicant his actions were not proper and that the document would be saved on the hard drive via auto save. Tr. 2/14/97 pp. 181-83. Applicant was aware classified processing was only to be performed on an approved automated information system but he did not think the information would be compromised by doing it quickly. Tr. 2/14/97 pp. 148, 160. Concerned by what he regarded as Applicant intentionally "cutting corners" to get the work done (Tr. 2/14/97 p. 214), co-worker B accompanied by another cubicle mate (co-worker D), informed their supervisor that Applicant had been working with classified information on an unapproved computer. The supervisor did not report the incident to security as he considered it a procedural problem, an administrative act in process that was corrected on the spot. Tr. 2/14/97 p. 218. App. Exh. A p. 14.

In about autumn 1995, Applicant inserted two or three classified Confidential numbers which identified radar power output into an Excel spreadsheet on an unapproved computer. Applicant realized that the numbers were classified but he thought if he did not reference the numbers to the program or the contract, the numbers would be meaningless. Co-worker B noticed the information pertained to classified transmitter output power and antenna gain numbers he was readily familiar with and immediately able to recognize them for the system they belong to. Suspecting this may not be proper, he informed Applicant who stopped processing while co-worker B contacted security. Advised by the security person responsible for automated information systems (Tr. 2/14/97 p. 53) that it was a "gray area" and should not be done, co-worker B told Applicant not to do it again. Applicant saved the classified processing on two diskettes which were erased by co-worker B. The two diskettes remained in Applicant's custody, unmarked and not safeguarded, until February 1996. Govt. Exh. 2; Tr. 2/14/97 pp. 115-16; 153; 182-84; 197. This incident was brought to the attention of Applicant's supervisor who did not report it to security because they cleaned the disk and took everything off the computer. Tr. 2/14/97 p. 219. Following the incident, co-workers B and D went through all the directories on Applicant's computer to determine if Applicant had improperly processed other classified information. They did not find any noticeable problems. App. Exh. A p. 22.

While discussing a new system with co-worker B on February 5, 1996, Applicant opened his desk drawer to look for the answer, caught himself, chuckled and smiled a little and said, "oh, wait, that's classified, that was in the safe." Tr. 2/14/97 pp. 185, 205; App. Exh. A. Co-worker B became suspicious that Applicant was keeping classified notes in his unlocked desk drawer. After Applicant left work for the day, co-worker B searched the file drawer in Applicant's desk for the program they had discussed earlier that day. He did not find any documents pertaining to that program, but did

find the notes containing Confidential radar systems information which Applicant had been referring to on a three times weekly basis for the last seven years. Co-worker B recognized the calculations themselves not as classified, except that on the top of each system, Applicant had listed the frequency range that each system operates in--two of the systems co-worker B considered classified. Tr. 2/14/97 p. 186. At that point, co-worker B completed his search, took the stapled set of working papers and secured it in the container approved for classified storage. Tr. 2/14/97 pp. 186-189. The following morning, co-worker B reported his discovery to their (his and Applicant's) supervisor. The supervisor turned the document over to the manager of Govt. security operations (Asst. FSO) at company A. Govt. Exh. 6; Tr. 2/14/97 pp. 32-33; 224. The Asst. FSO took the notes to the document control center and had them marked.(14) Tr. 2/14/97 p. 40; Govt. Exh. 6.

In accordance with industrial security program requirements, the Asst. FSO initiated an investigation. On February 6, 1996, she interviewed both co-worker B and the supervisor. Govt. Exh. 6; App. Exh. A. Co-worker B and the supervisor showed the Asst. FSO the information in the document which they felt was classified. The Asst. FSO marked these places with little sticky tabs. Tr. 2/14/97 p. 36. In a memorandum dated February 6, 1996 (Govt. Exh. 9), co-worker B confirmed his discovery of approximately twenty pages written in Applicant's distinctive hand, unmarked, on three pages of which classified frequency ranges were listed directly below the name of the corresponding radar system. In further discussions with co-worker B and the supervisor, the Asst. FSO was apprised of the two occasions in 1995 where Applicant had improperly processed classified information on an unapproved computer system. Govt. Exh. 6.

Applicant was asked to review the holdings within his desk and work area to ensure that no classified information remained unmarked or unprotected and to provide to security the two diskettes which he had in his custody on which he had improperly processed the classified information and which had been erased by co-worker B. He was advised that erasure of the information was not an approved method for destruction of magnetic media. In response to the Asst. FSO's request to explain the circumstances of the reported security violations (Tr. 2/14/97 p. 55), Applicant executed a memorandum of February 6, 1996, in which he stated the working papers were kept in a folder in his desk and used by him exclusively for reference purposes. As to the content of the notes, he related:

The papers contain formulas for calculating various radar power density values, which are an integral part of my job. Although the formulas themselves contain no classified data, a few of the calculations on certain added pages do contain numbers (operating frequencies of certain radars) which are classified. I never gave these papers to other people, nor did I ever make copies or take them out of the building. Because of negligence on my part, these papers were never properly marked.

He further indicated that he was in the process of checking all his unclassified papers and computer disks for any overlooked classified information. Govt. Exh. 10. The following day, Applicant informed the Asst. FSO by letter that he had thoroughly checked all the papers in his desk area and no other unmarked classified data existed. No apparent classified data was found on his "two floppy computer disks." App. Exh. A p. 9; Govt. Exh. 10 p.2. He returned the floppy disks which he had in his possession to security. On February 8, 1997, co-worker D, at the request of the security department, performed a hard disk wipe on the two computers used by Applicant. Govt. Exh. 8.

On February 7, 1996, the Asst. FSO provided the tabbed working papers to the chief scientist at company A to have the classification authenticated. Govt. Exh. 6; Tr. 2/14/97 p. 36. On initial review, the chief scientist based on his knowledge of radar systems from working in the area since 1959, noticed on one page of notes a set of calculations which could be applied to many radar range installations with a small change to one or more of the consonants in the radar system. He found at least one instance where the consonant was associated with a particular radar set which made it classified Confidential. While he found on initial review only one type of information which he determined to be classified, it was discovered on several pages of the document.(15) Tr. 4/4/97 pp. 35-36. The Asst. FSO interviewed Applicant sometime after the chief scientist determined there was Confidential information in the working papers(16) and prior to February 23, 1996. Applicant admitted to the Asst. FSO that he was aware the notes contained classified information. When questioned about his failure to mark or safeguard the notes, Applicant responded that the notes were kept in his desk and used by him for reference purposes only. Govt. Exh.6. On February 26, 1996, in accordance with industrial security requirements, the Asst. FSO submitted to DIS an initial report of the violations in which the Asst. FSO adjudged Applicant culpable of the following:

1. Failure to properly mark a Confidential classified document and floppy diskettes.

2. Failure to properly safeguard Confidential classified material and magnetic media.

3. Processed Confidential classified information on an unapproved AIS system.

4. Improper destruction of Confidential documents on magnetic media.

5. Willful disregard for security policies and procedures.

Govt. Exh. 6.; Tr. 2/14/97 65. Due to the circumstances of the violations and the fact that the violations had been ongoing for seven years, the FSO determined that the compromise of classified information could not be ruled out. Govt. Exh. 6.

By letter dated February 26, 1996, company A's FSO recommended to Applicant's immediate supervisor that Applicant be suspended from work without pay for three days and his access to classified information be suspended indefinitely. (Govt. Exh. 7). The manager of Human Resources at company A did not concur as such action would result in Applicant's termination from employment. During a meeting attended by the FSO, the Asst. FSO, the Human Resources manager, a senior security specialist, and Applicant's second level supervisor, decision was made to suspend Applicant from work for one week without pay. Tr. 2/14/97 p. 39. On March 14, 1996, Applicant was notified in writing that he was to be suspended from work without pay for five days from March 18 through March 22, 1996, due to his mishandling of classified information. On return to work on March 25, 1996, he would be required to be re-trained in the proper handling of classified documents and subjected to random spot checks by his managers and security. He was informed that any further occurrences of this nature could lead to his termination. Govt. Exh. 5. Following his five day suspension, Applicant returned to regular duties, to include accessing classified information.

On March 26, 1996, while reviewing documents he had stored on his work computer, Applicant discovered a trip memo he had written in about October 1995 that he thought might contain classified information pertaining to a new program involving electronic warfare equipment.[(17)] Applicant had a hard paper copy of the memo in his files as well as a floppy disk which he was certain contained a copy of the memo. Applicant brought the situation to the attention of co-worker B. They mutually agreed that the hard copy, the floppy disk, and the computer backup tapes should be immediately turned over to the security department. Tr. 2/14/97 p. 124. Since it was late in the day, co-worker B suggested that they render the floppy disk useless. Co-worker B then took a pen and poked a hole through the floppy. Tr. 2/14/97 pp. 200-01. Neither co-worker B nor Applicant realized that it was improper to destroy the disk in this manner.

On March 27, 1996, Applicant contacted the Asst. FSO and informed her that he thought there was a possibility that a memo he had generated and discovered on a floppy may contain classified information on a Secret level. He also indicated copies of the memo had been distributed to his supervisor, his second-level supervisor and co-worker E. The Asst. FSO contacted these three individuals and requested that they check their files for this memo and turn it over to her. On arch 29, 1996, Applicant provided the damaged floppy and backup tape to the Asst. FSO. Applicant indicated to the Asst. FSO on that date that he had punched a hole through the disk with a pencil so that it could not be reviewed. The following day, she received a copy of the memo from Applicant's second-level supervisor. Since she could not determine whether it contained classified information, she provided it to co-worker E, the resident expert at company A on the electronic warfare system. He could not determine if it was classified. She secured it in an approved container pending review of the memo for classification, which the Asst. FSO advised DIS would be requested from the user agency. Review of the damaged disk was not possible. App. Exh. A pp. 36-37.[(18)] On July 2, 1996, the DIS ISS was advised that a review of the document had been conducted by co-worker E, senior member of the engineering staff, who determined from the security classification guide that the trip memorandum contained Confidential information. Govt. Exh. 14; Tr. 2/14/97 pp. 79-80.

Applicant was requested to document the incident by the Asst. FSO. In a written interoffice memorandum dated April 2, 1996, Applicant explained that on March 26, 1996, while reviewing documents he had stored on his PC hard drive, he discovered a document pertaining to [the electronic warfare] system which has certain classified capabilities. He maintained that the document contained no classified information nor did it name the capabilities. However, it might be

possible for a knowledgeable person to surmise this capability from the manner in which the document was written. He maintained it was unintentional. Applicant stated that the document was originally saved on a floppy and then dumped to the PC hard drive which is connected to a tape back-up system. He indicated that he intentionally poked a hole through the floppy disk to render it unusable and took both the floppy and backups to security. Govt. Exh. 4.

As an -------- whose work with radar systems was integral to his job, Applicant would be expected to be aware of what was classified under the pertinent security guideline. Tr. 4/4/97 p. 71. As a cleared employee, Applicant had been given a small pamphlet titled *Security and You* (*See* Govt. Exh. 16) which explains how to mark, process and store classified information. In addition, the facility security manual, which specifies the procedures for the safeguarding and handling of classified information, was made available to cleared employees through their supervisors and Applicant had reviewed the manual. Company A publishes as well a newsletter which contains "security gram" articles updating employees on handling of classified information which Applicant reads. App. Exh. A; Govt. Exh. 2. Shortly after his return to work following his five day suspension in March 1996, Applicant was given a security briefing about the proper procedures for handling classified information. Govt. Exh. 2 p. 13. In addition to this formal security education, Applicant's co-workers B and D made efforts to help Applicant understand proper safeguarding procedure. Co-worker B, who is regarded as very security conscious, kept the facility security manual on his desk. On several occasions, he referred Applicant to specific provisions of the manual. App. Exh. A p. 23.

In addition to his work in the unsecured area, Applicant was involved in a special access program from October 1993 to March 1996. On October 20, 1993, he signed a program indoctrination agreement. Govt. Exh. 13. On October 23, 1993, he received his initial security briefing to work in the secure area. As part of his briefing he was required to review the security manual, was told how to handle classified information, and apprised of the proper use of a secure telephone. While working in the special access area, he was informed of the proper procedures for creating, marking, and making classified documents accountable. He received written instructions on the circumstances in which he could leave a document out in a secured area and advised he had ninety days in which to enter a document into accountability. App. Exh. A p. 26. He was re-indoctrinated about security requirements within the special access program on August 22, 1994 and on August 11, 1995. Govt. Exh. 13. On one occasion between October 1993 and 1994, while working in the secure area, Applicant failed to lock up classified material before he left. The security monitor found the papers and secured them. App. Exh. A p. 28. On two separate occasions, Applicant created a classified document and failed to make it accountable within the ninety day allowable time period. App. Exh. A p. 29. Applicant did not receive a security violation or an administrative deviation regarding these incidents. On March 15, 1996, he was de-briefed from the special access program as his project there was completed. Govt. Exh. 13.

On April 24, 1996, Applicant was interviewed by Special Agent C of the Defense Investigative Service concerning the reported security violations. As reflected in a signed, sworn statement attested to as being accurate and true as written, with respect to his processing of a confidential table on an unapproved automated information system, Applicant admitted he knew at the time he was not following proper security procedures, but that his project was due that particular week and could not be completed without the table. He also acknowledged his knowing insertion of classified radar output information into an Excel spreadsheet in fall 1995 on an unapproved computer. He thought that if he did not reference the program or contract, it would be meaningless and not an improper security procedure. Concerning the disk wipe of the diskettes by co-worker B, Applicant related he had believed it was the proper way to erase the classified information. He indicated he did not realize at the time that any use of classified numbers on an unapproved computer was improper. With respect to the classified working papers which he kept unsecured in his desk for seven years, Applicant stated that he inserted two sets of numbers on two pages without representing the pertinent contract but that on the other eighteen pages, there were references to radar set #1 once or twice. While he had believed that because the numbers were not on the same page as the identifying contract it would not be a problem, he indicated he now understood it was not the correct way to handle the classified information. Govt. Exh. 2 pp. 2-7. He attributed his violations for which he was suspended to "complacency." Govt. Exh. 2 p. 12. Regarding the trip memorandum which he recently discovered, Applicant related that on March 26, 1996, he poked the hole in the disk that contained the memo to render it unusable. He did not think at the time that his action was improper. Govt. Exh. 2 p.8. Applicant intentionally lied to the Agent when he told her he punched the hole in the disk because he was already in a lot of trouble and did not want to bring co-worker B into it. Tr. 2/14/97 p. 125. Of his reported failure to make documents accountable on two occasions while working on the special access program, he stated it was not intentional; that he simply forgot. Govt. Exh. 2 p. 10.

On July 16, 1996, Applicant was reinterviewed by Special Agent C concerning the extent and nature of the classified engineering notes found in his desk on February 5, 1996 by co-worker B. Applicant indicated that he never had an opportunity to count his notes and had believed they amounted to twenty pages. He acknowledged they could be thirty pages in length and indicated that he had mistakenly believed that a substantial portion of the notes had been given to him by the co-worker.

Infrequently, security in the last year has performed spot checks to see if classified material was being stored on or around Applicant's desk. No problems have been detected. Tr. 2/14/87 p. 56. For eight months to a year following his discovery of the classified information in Applicant's unlocked desk, co-worker B continued to share a cubicle with Applicant and he continues to work with Applicant on numerous projects in their new location. Applicant has had the opportunity to access classified information on a daily basis. Several times over the past year, he took classified materials out of state to make classified presentations to the Government. Tr. 4/4/97 pp. 97-98. During the course of discussing their common work in the past year, Applicant has indicated to co-worker B "that he does have a sense of identifying the obviously classified and questioning some of the new systems that [they're] currently dealing with at this time." Tr. 2/14/97 p. 208.

Applicant has been consistently rated as a ---------- since his employ at company A. Govt. Exh. 11. Applicant's first level supervisor recommends Applicant for continued access to classified information and regards Applicant as much more security conscious since the violations. Tr. 2/14/97 p. 220. Applicant is considered by his second level supervisor to be a dedicated, hard worker who has learned from his mistakes. App. Exh. A pp. 12-13.

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 doubt 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:

(1) were inadvertent

PERSONAL CONDUCT

Conduct involving questionable judgment, untrustworthiness, unreliability or unwillingness to comply with rules and regulations that could indicate that the person may not properly safeguard classified information.

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

(3) deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official . . .or other official representative in connection with a personnel security or trustworthiness determination.

Conditions that could mitigate security concerns include:

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 established its case with regard to criteria K and E.[(19)]

The Government has an unequivocal need to protect classified information within the defense industry. Only those applicants who demonstrate the appropriate good judgment and reliability in the protection of such information will be granted the privilege of a security clearance. The evidence establishes that Applicant in about 1989 drafted a document (some thirty-two pages in length)[(20)] containing formulas and calculations which he used regularly in his work on classified radar contracts at company A and that on multiple pages (no more than eight), he knowingly included confidential information.[(21)] Applicant did not apply any classification markings to the document. His action in that regard is found to have been in deliberate disregard of his known obligation, as a cleared employee, to properly mark working papers which contain classified information. While Applicant initially testified that he believed the information was not classified if he did not mark it (Tr. 2/14/97 p. 141) and that he did not realize he had to mark his working papers

(Tr. 2/14/87 p. 157), he admitted he had been briefed in the special access program that he had to mark a document generated by him if is contained classified information. Moreover, Applicant admitted to having a copy of the security handbook *Security and You* which is clear on the marking of classified working papers:

Classified Working Papers

All notes, drafts, and working papers must be dated, have the overall classification conspicuously marked at the top and bottom, front and back on the outside of the document. Each internal page must be conspicuously marked top and bottom to reflect the highest level of classified information appearing on that page.

Govt. Exh. 16 p. 18. This requirement is consistent with the Industrial Security Manual for the Safeguarding of Classified Information, DoD 5220.22-M, dated January 1991 (hereafter ISM) and the National Industrial Security Program Operating Manual, DoD 5220.22-M, dated January 1995 (hereafter NISPOM) which superseded the ISM.[(22)] ISM ¶4-102 c. and NISPOM ¶4-102 c. impose the responsibility on the individual employee who copies or extracts classified information from a document to mark the new document with the same classification marking as applied to the source document. ¶4-201 of both manuals make it clear that all classified material be marked to the fullest extent possible to ensure it is afforded the necessary safeguards. The working papers are required under both the ISM and NISPOM to bear identification markings (¶4-202), to include the name and address of the facility and date of preparation; an overall conspicuous marking of the highest level of classified contained in the document (¶4-203); interior page markings with the highest level of classified on the page noted or the designation "Unclassified" if appropriate (¶4-204); portion markings in a manner that eliminates doubt as to which of its portions (sections, parts, paragraphs) contain or reveal classified information (¶4-206); a marking noting the source of the classification (¶4-208). Furthermore, ¶4-213 of the NISPOM sets forth the mandates for marking information that would otherwise be unclassified when standing alone but classified will be revealed when they are combined or associated. Applicant violated all these provisions when he failed to mark his papers with the appropriate classification markings.[(23)]

Applicant referred to this unmarked, Confidential document on a regular basis (three times a week) until it was discovered in his unlocked desk by co-worker B on February 5, 1996.[(24)] When he was not referring to these engineering notes, he kept them in his unlocked desk despite the fact he had an approved classified storage container three feet from his desk. Applicant told DIS Special Agent C that he never thought to place them in the storage container. He also claimed that he did not think he had to secure his notes as the information was published in unclassified, open sources. Co-worker B testified that leaving classified unprotected in his desk was "out of character" for Applicant (Tr. 2/14/97 p. 206). Applicant accessed classified material with regularity on the job and apparently secured that information properly. Given he knew the document had classified numbers in it, his failure to secure the document is viewed also as a deliberate disregard of known security obligations. The company A security handbook (Govt. Exh. 16 p. 19) as well as ¶5-306 of the ISM and ¶5-304 of the NISPOM specify that confidential material must be stored in the same manner as Top Secret or Secret material with the exception that no supplemental controls are required.[(25)] Under the ISM Top Secret material was to be stored in a GSA approved security container or an approved vault, with supplemental controls. ISM ¶5-302. With the NISPOM, it could also be stored in an approved closed area with supplemental protection. NISPOM ¶5-302. Secret material under ¶5-304 of the ISM and ¶5-303 of the NISPOM could be stored in an approved security container or vault (or under NISPOM only approved closed area) authorized for storage of Top Secret or in a security cabinet or strongroom in either a safe or steel file cabinet with prescribed locking mechanisms. While there is no evidence that the information was compromised, the possibility of an uncleared person gaining access cannot be completely discounted as Applicant's desk was in an open area, his desk was kept unlocked and uncleared personnel, to include cleaning crews, had access to the area. Company A's security handbook, moreover, makes it clear that classified material is to be placed "when not under the constant surveillance of an authorized person, in a container approved by [the] Security Office and secured by a three-position, changeable combination padlock or built in combination lock." Govt. Exh. 16 p. 37.

On one occasion in summer 1995, Applicant knowingly processed classified information on an automated information system (computer) which had not been approved for such processing. In a hurry because his project was due, Applicant typed Confidential numbers into a table on an unapproved computer. At the time, Applicant did not think the information would be compromised by doing it quickly and saving it to a floppy. Even assuming Applicant did not

realize the import of the auto save function, he was aware that he should not have been using an unapproved computer for the work. Company A's security handbook provides "classified material may not be processed or stored on any computer system without specific, prior written approval of the United States Government." Govt. Exh. 16 p. 9. His unapproved processing was also in violation of ¶8-100 of the NISPOM which requires that computer and networking systems be operated so that the information is protected against unauthorized disclosure or modification.[(26)]

Subsequent to this incident, Applicant in about fall 1995 inserted on another occasion two or three Confidential numbers into an Excel spreadsheet using an unapproved computer. Applicant realized that the numbers were classified, but thought there would be no problem if he did not reference the numbers by contract or program.[(27)] While co-worker B readily identified the information as Confidential, there was sufficient question about the propriety of Applicant's actions for co-worker B to contact security. Whereas Applicant was aware that the numbers were classified, at a minimum he was grossly negligent in not checking with his supervisor or security personnel before he inserted the information.[(28)] On being apprised by security that such processing was improper, Applicant saved the processing on two diskettes[(29)] which were immediately erased using Norton disk wipe by co-worker B. While neither co-worker B nor Applicant realized that the method of erasure was not sufficient to ensure destruction of the classified information on the diskette, they violated their company's established destruction procedures. As set forth in *Security and You,* "classified materials can only be destroyed by the appropriate Classified Document Control Center (CDCC) or Security Service Center (SSC)." Govt. Exh. 16 p. 19. Destruction requirements for magnetic media under the NISPOM specify that the media be sanitized in accord with authorized sanitization procedures (¶8-302 e.), that all markings and labels removed before media can be declassified (¶8-302 f.) and that the media must be sanitized and declassified before release from continuous protection (¶8-302 g.). After erasure, the two diskettes remained in Applicant's custody until February 1996 and were not safeguarded. Applicant's failure to secure the floppies in the storage container was not intentional, but due to his misunderstanding that the classified information had been properly erased from the diskettes.

In determining the current security significance of the aforesaid violations of the requirements for handling and safeguarding classified information, this Administrative Judge must consider the Adjudicative Guidelines pertaining to security violations set forth in Enclosure 2 to the Directive. Although the possibility of compromise cannot be completely discounted because the classified working papers referred to in subparagraphs 1.a. and 1.b. of the SOR remained unprotected for some seven years in an unlocked desk, there is no evidence that information was disclosed to unauthorized persons. Disqualifying condition (DC) 2. is apposite, however, as Applicant committed multiple violations of security requirements, some deliberate and others negligent. The most serious violations involve the deliberate insertion of classified material in his working papers and his intentional failure to mark and secure them for the next seven years. Applicant's desire to have ease of access to his engineering notes was placed before his obligation to safeguard Confidential information. Known security responsibilities with regard to AIS classified processing also were sacrificed to get a project done timely during summer 1995. After Applicant had been reminded of his obligations with regard to processing classified information only on an approved computer, Applicant in the fall entered in a spreadsheet on an unapproved computer classified information which was recognizable as Confidential by co-worker B. Although the company A security handbook clearly states that no classified information is to be processed or stored on a computer unless it has been approved by the United States Government, there was sufficient uncertainty about Applicant's entry of classified numbers in the spreadsheet given the information was not associated with the specific program for co-worker B to contact company A's security department. Applicant was negligent in not checking with security or his supervisor himself before he entered the Confidential data.

Of the four potentially mitigating conditions (MC), only MC1. (inadvertent violations) applies, and that is only with regard to the failure to mark the floppy diskettes on which he saved the spreadsheet, and his subsequent failure to secure them because he assumed all the classified information had been deleted. While Applicant and co-worker B did not understand that Norton disk wipe was not a proper method of destroying the information, they were negligent in not presenting the floppies to security for destruction which is required by company security procedures. This Administrative Judge is not persuaded that MC 2. (isolated or infrequent violations) works to Applicant's benefit, notwithstanding the limited number of violations when compared to twelve years of regular access. First, the circumstances surrounding the engineering notes reflect an ongoing, repeated failure to mark and secure the document over a substantial period (seven years) of time. Second, his record of violations is not limited to the classified working papers but also includes improper use of automated information systems.[(30)] Applicant's contention that the violations

were due to improper or inadequate security training (MC 3.) is based largely on his own testimony that he received a general security briefing when he was first employed which did not include training in handling of a disk including classified information and that subsequent briefings lacked specificity, as well as on the opinion of Applicant's supervisor that the security office was at fault for not being more definitive in regard to security training. (See App. Closing pp. 11-12; 88-89). Following the incidents involving the unauthorized processing of classified information on an unapproved computer, Applicant's supervisor requested security provide a refresher course for Applicant. He was told that Applicant could attend the normal security course.(31) The security office cannot be faulted for Applicant's failure to get additional security training when the course offered was rejected. With respect to the quality of the security training at the facility, co-worker B testified to his lack of awareness prior to the incident as to the existence of contract specific security classification guidelines (Tr. 4/4/97 pp. 104-05) and to having received recently only briefings pertaining to the releasability of project information to a foreign country (Tr. 2/14/97 p. 202). Even so, he has been employed by the facility since June 1989 and shown by his actions to be security conscious. With the assistance of co-worker D, he made an effort prior to February 1996 to educate Applicant in his security responsibilities, by directing Applicant at times to the facility security manual. In addition, Applicant received a number of briefings in the special access area which should have heightened his security awareness. As a cleared employee, moreover, Applicant has an affirmative obligation to comply with security requirements promulgated for the safeguarding and handling of classified information. Applicant admitted he had access to the facility security manual and had his own copy of the facility's security handbook. The violations which engender the greatest concern reflect not a lack of awareness of requirements, but a disregard of known security obligations. It is further noted that when interviewed by DIS Special Agent C regarding the security infractions, Applicant attributed the violations to "complacency," not to inadequate training.

Security clearance decisions are not designed to punish applicants for past wrongdoing, but involve an assessment of future security risk. After his suspension from work for five days without pay, Applicant was allowed to return to regular duties on March 25, 1996, to include accessing classified information on a regular basis. There have been no security incidents during that time. Furthermore, co-worker B, who no longer shares a cubicle with Applicant but has had the opportunity to work with Applicant on classified projects since March 1996, testified Applicant "does have a sense of identifying the obviously classified and questioning some of the new systems." Whether or not an applicant has rehabilitated himself depends on recognition and acknowledgment of his wrongdoing and demonstration by conduct over a period of time that he is willing and able to adhere to applicable laws and regulations. Applicant's unblemished record with regard to handling classified information over the past year is laudable, but it must be balanced against a record of violations which includes subjecting confidential information to possible compromise for seven years. Applicant testified that he would never process classified material on an unapproved computer again and that anything that is "gray," he now considers "black." Security concerns nonetheless persist because of the seriousness of his deliberate disregard of known security regulations and his failure to admit to the intentional nature of some of the violations. At the hearing conducted on February 14, 1997, with respect to the notes found in his desk, Applicant testified that there was classified on only two pages, one of which was a classified paper on his desk which inadvertently got clipped in. If this was indeed the case, the other classified paper should have borne the appropriate markings. While he did not have the benefit of recent review of the notes, these working papers were not placed in his desk and left there forgotten for seven years. Rather, he referred to them three times per week in his work. He also testified that he believed at the time the information was classified if it was marked as such and unclassified if he wrote it down without appropriate classification markings. It is simply not credible that one with twelve years of regular access would lack such a fundamental understanding of the nature of classification. Furthermore, Applicant asked to work without pay during that time he was suspended from work which reflects a lack of appreciation for the gravity of the violations. Tr. 2/14/97 p. 161. In his most recent performance evaluation, which he signed on March 26, 1996 (Govt. Exh. 16) Applicant indicated his immediate career goal was to become more attentive to the proper handling of classified material. The record is silent as to actions taken on his own initiation, if any, to familiarize himself with the facility's security manual and the NISPOM. After considering the seriousness and extent of his criterion K conduct, his evidence in reform falls short of overcoming the Government's legitimate security concerns. Accordingly, subparagraphs 1.a., 1.b., 1.c. and 1.d. (with respect to the processing of classified on an unapproved system only) are resolved against him. Subparagraph 1.f. does not represent a separate violation, but rather is the administrative sanction which was taken against Applicant by his employer for failing in his security responsibilities. That allegation is found against him because it references his record of security violations.

With respect to the Criterion E allegation which was added at the hearing, the evidence substantiates that in October

1995, Applicant completed a trip memorandum which he discovered during a search of his desk and files on March 26, 1996. Suspecting that it might contain classified information, Applicant notified co-worker B and together they decided to turn both the printed copy of the memo and the magnetic media on which it was generated (floppy and backup tapes) to security. In an effort to render the diskette unreadable, co-worker B in Applicant's presence took a pen and poked a hole in the floppy. When interviewed by both the Asst. FSO and DIS Special Agent C about the incident, Applicant intentionally misrepresented the circumstances of the floppy's destruction in that he indicated he punched the hole in the floppy disk in order to render it unusable. DC 3. (deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official in connection with a personnel security determination) under the personal conduct guidelines must therefore also be considered. Applicant submits that while he made a false statement, the fact misrepresented was not in itself an actionable security violation and therefore not the type of activity intended to be covered by Criterion E. This Administrative Judge found there was no malicious attempt to destroy the classified information when co-worker B poked the hole in the disk. Rather, the intention was to render the disk unreadable in order to preclude unauthorized access to classified information. Nonetheless, the disk was not destroyed in a manner consistent with either the facility's security handbook or the NISPOM. As set forth in *Security and You,* "classified materials can only be destroyed by the appropriate Classified Document Control Center (CDCC) or Security Service Center (SSC)." Govt. Exh. 16 p. 19. Destruction requirements for magnetic media under the NISPOM specify that the media be sanitized in accord with authorized sanitization procedures (¶8-302 e.), that all markings and labels removed before media can be declassified (¶8-302 f.) and that the media must be sanitized and declassified before release from continuous protection (¶8-302 g.). Although Applicant and co-worker B were not certain there was classified information in the memo, and hence on the diskette, where they suspected it to be classified, they had an obligation to protect it as such until learning otherwise. Therefore, the manner in which the disk was rendered unreadable was in negligent violation of pertinent security requirements. As testified to by the Asst. FSO, she could not confirm that the copy of the classified trip report was on the disk because a hole had been punched in it.

Furthermore, although the false statement was made to protect co-worker B and not to impede the Government's investigation into the reported security violation, a malicious intent is not required. For purposes of criterion E, it is enough that a false statement was deliberately made and that the false statement was material. In this case, the misrepresentation had the capability of influencing the Government agency's investigative decisions in determining the course and direction of the inquiry involving a reported possible security violation.

Of the seven listed mitigating conditions, only four have potential applicability. As discussed above, the information was pertinent to a determination of Applicant's judgment and reliability. The Government must be able to rely on the representations of those to whom it has entrusted the Nation's secrets. Favorable consideration of MC 2. is likewise precluded because of the recency of Applicant's false statement which he made on April 24, 1996, within a year of the hearing in this case. With respect to the prompt, good faith effort to correct the facts required for MC 3., Applicant had an opportunity to correct the record when he was reinterviewed by Special Agent C on July 16, 1996 regarding the extent and nature (whether they were largely drafted by him and consisted of 30 vice 20 pages) of the engineering notes which were found in his desk on February 5, 1996. Applicant did not correct the record with the Government until the February 14, 1997 hearing. Apparently, even co-worker B was unaware that Applicant was claiming responsibility for punching the hole until just prior to the hearing on February 14, 1997. Nor is there any evidence that misrepresentation was due to the improper advice of an authorized person. While the failure to satisfy any of the corresponding mitigating conditions is not necessarily dispositive, Applicant's lack of credibility at the hearing concerning the violations compounds the concerns engendered by his criterion E conduct.[(32)] An adverse finding is therefore warranted with respect to subparagraph 2.a. of the SOR as amended.[(33)]

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.: Against the Applicant

Subparagraph 1.b.: Against the Applicant

Subparagraph 1.c.: Against the Applicant

Subparagraph 1.d.: Against the Applicant

Subparagraph 1.e.: withdrawn

Subparagraph 1.f.: Against the Applicant

Paragraph 2. Criterion E: AGAINST THE APPLICANT

Subparagraph 2.a.: 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 February 5, 1997, the undersigned received an "Agreement and Stipulation" signed by Department Counsel on January 2, 1997, and by counsel for Applicant on January 31, 1997, in which the parties stipulated to the admission and pre-hearing consideration of the sixteen Government exhibits appended to the document. On February 7, 1997, Department Counsel forwarded another copy of the second page of the stipulation which bore the signature of Applicant, dated February 7, 1997, in addition to the signatures of Department Counsel and Applicant's counsel. That copy of the stipulation agreement which was signed by Applicant and the respective legal counsel was marked and entered into the record as Joint Exhibit 1. Although not included in the "Agreement and Stipulation," also forwarded on February 5, 1997, was a Defense Investigative Service (DIS) Report of Investigation (ROI), dated August 5, 1996. On February 7, 1997, the undersigned received through Department Counsel portions of a handbook submitted by the Applicant for pre-hearing consideration. Department Counsel having no objection, the ROI and Handbook were admitted as Applicant Exhibits A and B, respectively.

2. Applicant, through counsel, had no objection to the amendment and requested no additional time to respond. He denied the allegation on the ground that he had no intent to deceive the Government. (Transcript 2/14/97, pp. 173-74).

3. This Administrative Judge therefore will render no formal findings with respect to that subparagraph.

4. As confirmed by Applicant's performance evaluations (Government Exhibit 11), corporate ownership of the facility has changed three times since his hire, but it has remained a defense contracting concern.

5. On April 24, 1996, Applicant indicated to DIS Special Agent C that he obtained twenty pages of notes from the co-worker, to which in 1989 he began to add radar frequency information. (Govt. Exh. 2). The record evidence reflects, however, that only two pages of the thirty-two page document found in Applicant's unsecured desk were in this co-worker's handwriting, the remainder was in Applicant's hand. (App. Exh. C). Applicant admitted at the hearing that the bulk of the document came from him. Tr. 2/14/97 p. 138.

6. On review of Applicant Exhibit C, two of the pages appear to be the same. Both of these pages contain information classified at the Confidential level. *See also* Tr. 4/4/97, p. 49.

7. The chief radar scientist at company A reviewed the notes and found classified information on eight of the thirty-two pages. Tr. 4/4/97, pp. 59-68. As noted in footnote 6, two of the pages appear to be the same. Whereas there was no precise accounting of the document taken from Applicant's desk at the time it was found (neither co-worker B, his supervisor, or the Asst. FSO counted the pages), the original document may well have been 31 pages vice 32 with one page copied twice. With respect to the electronic warfare system information, the chief scientist testified credibly that

the frequency range over which the warfare device operates and the frequency of this device is certainly classified. Tr. 4/4/97 p. 52.

8. The confidential information entered in the working notes, at least with respect to the frequency information pertinent to radar set #1, was basic to Applicant's work (*See* Tr. 4/4/97 p. 68) and immediately recognizable as classified by co-worker B when he discovered the papers in Applicant's desk on February 5, 1996.

9. According to co-worker B, Applicant (at least prior to February 1996) became confused when pieces of outdated information that are still classified become incorporated into a related contract making that contract classified. Applicant believed that he no longer had to follow the contract guidelines and that supervisors had to explain to him that it didn't matter what other agencies did, he still had to follow the contract guidelines. App. Exh. A p. 19.

10. It is not obvious that co-worker B and Applicant are talking about the same number. Applicant contested the classification of a frequency number while co-worker B spoke of one power output value. At best, this would invalidate the classification assessment of the one power output value. There was other Confidential information in the document.

11. Applicant testified that he agreed with the chief scientist's assessment as to the two numbers identified as classified, but as to the other pages which were marked as classified, they were checked and determined to be not classified. Tr. 2/14/97 p. 143. Neither the Asst. FSO or chief scientist confirmed Applicant's testimony. Furthermore, it is noted that Applicant's claim to the classified material not appearing on the first two pages was made on direct examination and in connection with a false denial of any knowledge that he was inserting classified material in his notes:

Q Did you at certain times insert certain numbers on that document, which are now being characterized as being classified?

A Yes. The way that happened was a while back, I was working on a classified document, and I believe that somewhere along the line inadvertently, those numbers got clipped in with the document. That was for--I think what we're talking about, two pages here, is my recollection. One was inadvertently put in a long time ago. It just--there were papers on my desk. It was a classified paper on my desk. And then next to it, there must have been the document in question, which was filled with unclassified information. Somehow a long time ago, I guess six or seven years ago, it got clipped in with the unclassified information and it remained there. That was one page. Then the other page, which contained one of the frequencies in question, I believe I wrote that in there a while back with the intent that, number one, I don't believe that I had it marked. It was buried in a formula, which I believe that nobody would really ever pick out. Also, I had seen this number passed around in several other documents that were put out by the [user agency]. These are unclassified documents. Tr. 2/14/97 pp. 117-18. . .

Q So that the number that you wrote in there, which we were told is classified, is a number that's found on an unclassified document?

A Yes.

Q And the other--

A Not just this document, but I mean, there are other documents also that list the number that are unclassified.

Q So at that time, you didn't think that you were putting classified information in that document?

A No.

Q And I believe you testified that the other information that was in there that was considered classified was information which inadvertently got included in that group of papers. Is that correct?

A That was inadvertently clipped in there somehow years ago, yes.

Tr. 2/14/97, pp. 120-21. While Applicant did not have the benefit of recent review of his notes prior to his testimony at

the first hearing, his claim that classified material was inadvertently included in the notes is not credible. After reviewing the notes (App. Exh. C) and the testimony of the chief scientist, the Asst. FSO and co-worker B, it is apparent that none of the pages in the thirty-two document contained any classification markings of any kind when they were found in Applicant's desk. If a page from a classified document had been inadvertently clipped in as Applicant claimed, it should have borne the proper classification markings. His credibility is undermined by his efforts to downplay the extent of classified information he knowingly inserted in his notes.

12. The testimony supports a clear finding of classified information at a minimum on the first page as well as on two other pages where Confidential information pertaining to the electronic warfare equipment appears.

13. Applicant initially testified that he believed the information was classified if it was so marked and unclassified if he just wrote it down without the appropriate classification marking. Tr. 2/14/97 p. 141. He also indicated that he did not understand that he had to mark his working papers as classified. Tr. 2/14/97 p. 157. Applicant subsequently admitted during briefings for special access programs he had been told if he generated a document that contained classified information, he had the obligation to mark it. Tr. 2/14/97 p. 158. He went on to attribute his failure to mark the document to forgetfulness. Tr. 2/14/97 p. 158. It is clear to this Administrative Judge that he intentionally did not mark the document because he wanted to keep it in his desk for easy reference and application of the appropriate marking would possibly have alerted someone in the company to his ongoing security violations.

14. At the hearing held on February 14, 1997, the Asst. FSO testified the document was approximately 20 pages but that she did not count them. Tr. 2/14/97, p. 35.

15. In her initial report of the violation to the Defense Investigative Service (Govt. Exh. 6), dated February 26, 1996, the Asst. FSO indicated there was classified information on "a few" of the pages. Asked at the hearing to reconcile this with the chief scientist's statement during his interview with DIS that on initial review he found one item which was classified, the Asst. FSO testified that the chief scientist told her there was classified on a few pages. While the chief scientist confirmed he told DIS Special Agent C on March 22, 1996, that there was one page a set of calculations which could be applied to many radar range installations with a small change to the consonants which he considered classified, he also testified that there were several pages in the document that have references to a radar set some of whose primaries he believes to be classified. Tr. 4/4/97 p. 35. He subsequently testified in clarification that he caught one type of information that was reflected on several pages. Tr. 4/4/97 p. 68.

16. The chief scientist reviewed the document several times at the request of the security department. It is not clear in the record when these subsequent reviews took place. The Asst. FSO testified on 2/14/97 as follows:

A I placed the tabs on them and showed them to [the chief scientist], and he did say, yes, they were classified in accordance with the [user agency] instruction for general radar.

Q And you showed [Applicant] what?

A I showed [Applicant the chief scientist's] outcome of the classified material.

Q And what did [Applicant] say to that?

A He agreed it was classified confidential.

Q Do you recall how many pages we're talking about that contained this classified information?

A I believe it was five or six pages. As he went through them, there may have been one piece of classified on each page or more than one on each page.

Tr. 2/14/97 p. 38. On cross-examination, she indicated, "[The chief scientist] went through each page that we suspected classified material to be on. There may have been one or two incidents where it was not classified, but there were at least five to six that he did mark confidential, the C in parens that's required by the Department of Defense marking." Tr. 2/14/97 pp. 63-64. In clarification of an apparent conflict in her testimony with the account of the chief scientist to DIS

of March 22, 1996, she testified, "We set up a second date with [the chief scientist] with the actual general radar guide, the [user agency] instruction, and he applied that to the full contents of the document. And then it was recognized that five or six other items were classified confidential." Tr. 2/14/97 p. 65. She stated that the second meeting occurred after Applicant requested his notes back. It had not been properly marked at that time, and she took the document back to the chief scientist and he went through it again and marked it. Tr. 2/14/97 p. 67. The chief scientist testified on April 4, 1997, he met with the Asst. FSO several times, once shortly after February 6, 1996 where he reviewed the document against his general knowledge of the security guidelines and that to his recollection the document at that time was not tabbed. He went on to state that there was a subsequent meeting where he was given a tabbed document but he could not recall the date except that it must have occurred after his interview (of March 22, 1996) with the DIS Special Agent. Tr. 4/4/97 pp. 54-55. In assessing the classification level, he indicated he used the general guidelines under which they had been operating. Tr. 4/4/97 p. 56. The Asst. FSO on April 4, 1997 testified that the chief scientist's second review took place sometime in between the start of the initial investigation and the submittal of the final report to DIS. Tr. 4/4/97 p. 75. The final report is not in the record. She indicated that the second meeting with the chief scientist would have occurred prior to the date Applicant was suspended (Tr. 4/4/97 p. 78) which would have been sometime prior to March 18, 1996. The discrepant testimony on when the chief scientist reviewed the document is not especially significant. The significant facts are that there was classified information in the document which was not marked as such and that Applicant knew there was confidential information in the working papers.

17. This was a new system and issues had arisen before about classification. According to co-worker B, whether or not something was classified tended to change sometimes so there was often a need to refer to the program manager to request clarification. Tr. 4/4/97 p. 199. Applicant indicated that at the time he typed the memorandum, he did not realize he was typing classified information:

At the time that I typed it a year ago, I did not--at that time, I did not think at all that it was a classified document. After working on the project more and more, you kind of learn more and more about systems. And when I discovered this document later, from what I knew then, I thought maybe I better turn it in to make sure--you know to have security try to find out if it was, in fact, classified.

Tr. 2/14/97 p. 123. While the Asst. FSO testified co-worker E, the expert in the company recognized the memorandum as confidential on first look, co-worker E did not come forth with a definitive opinion on the classification until July 1996. See Govt. Exh. 14. Applicant's testimony that he did not realize he was writing a classified memorandum is regarded as credible.

18. The Asst. FSO testified on February 14, 1997, that she had a paper copy of the memo before Applicant brought her the disk and that Applicant's supervisor had apprised her of the trip report that he believed contained classified information. She further testified that she within a few days had a meeting with Applicant's second level supervisor and co-worker E and that co-worker E said that the memo contained confidential information. Tr. 2/14/97 pp. 79-80. Her testimony is at variance with what she told the DIS Special Agent in April 1996. Questioned about her prior interview, the Asst. FSO testified that the DIS investigator's account was not correct because co-worker E had determined the memo contained classified material. When confronted with DIS' repeated requests from April through June 1996 for a report on the incident and her response that she would not be filing one until she was provided specific information as to whether the document was in fact classified, the Asst. FSO responded, "I did not have a sheer determination that was classified information." Tr. 2/14/97 pp. 82-84. Asked on cross to confirm that as of June 27, 1996, she still did not know the information was classified, the Asst. FSO testified, "[co-worker E] had not got back to me, even though I had tried to contact him several times." While the Asst. FSO's account to the DIS Agent is considered more reliable given it was contemporaneous with the events and is consistent with other evidence of record, this Administrative Judge is not persuaded that the Asst. FSO intentionally lied during the hearing.

19. The Government's case was not based solely on the testimony of the Asst. FSO (which was inconsistent at times) and the DIS ISS (who lacked first hand knowledge of the events), but it also included documentation, to include Applicant's signed, sworn statements.

20. *See* Footnote 7.

21. At least with respect to the frequency information which co-worker B on initial review recognized as classified Applicant cannot reasonably claim that he did not realize the information was classified at the time he wrote the document. This information was basic to Applicant's work.

22. Applicant had an ongoing obligation to see that the materials were appropriately marked. Hence, both the ISM and NISPOM apply as his violation spanned the 1989 to 1996 time frame.

23. The Government also alleges that Applicant violated ¶4-311 of the ISM, which provision requires automated information system (AIS) removable information storage media and devices bear clear external markings. The Government did not prove that the working papers were ever on a floppy or entered into the computer hard drive.

24. The Government alleges in SOR subparagraph 1.a. that the document was discovered on February 6, 1996. That was the date on which co-worker B notified his supervisor of his discovery. That pleading defect is not fatal to the Government's case. Applicant was placed on adequate notice and there is no dispute in this case as to which document subparagraphs 1.a. and 1.b. refer.

25. The Government also alleges that the failure to secure the notes was in violation of ¶8-309 c. of the ISM and ¶¶8-302a. and 8-302.b of the NISPOM. These sections pertain to storage of classified AIS media. As noted in footnote 23, above, the Government did not prove that Applicant entered these notes or any portion thereof in his computer or on a floppy. The notes were handwritten and there is no reason to presume they were on a disk. The Asst. FSO's testimony found at pages 67 to 73 of the February 14, 1997 proceedings does not establish the notes were ever entered on an AIS.

26. The Government further alleges Applicant's processing on an unapproved computer was in violation of ¶8-102 b. and 8-200 a. of the NISPOM, neither of which directly apply to Applicant. ¶ 8-102.b. sets forth the responsibilities of the Information Systems Security Representative. There is no evidence that Applicant was the AIS representative for company A. ¶8-200 requires the contractor to obtain written accreditation from the cognizant security agency prior to processing classified information on AISs. There is no evidence that Applicant had an obligation to obtain that accreditation. Rather, accreditation was apparently obtained for the computer which Applicant attempted to use initially.

27. In addition to violating ¶8-100 of the NISPOM by failing to ensure adequate protection of the classified processing, there is no evidence that Applicant marked the information on the diskettes consistent with the requirements of ¶4-102 c., 4-204 (page markings), 4-206 (portion markings), 4-208 (source markings), 4-213 (compilations markings), and 5-205 (marking classified working papers). The Government also alleges Applicant did not mark the spreadsheet as a working paper in accordance with the requirements of ¶5-205. On its face, ¶5-205 a. does not apply as the information was confidential, not top secret. Where this spreadsheet was a document in process, it is considered a rough draft or working paper which would fall under ¶ 5-205 b.

28. Applicant submits it was a gray area. While co-worker B contacted security personnel to determine whether it was improper to enter the classified numbers in the spreadsheet, it is also noted that co-worker B recognized the information as classified transmitter output power and antenna gain numbers, and was readily able to ascertain which system they belonged to.

29. Pursuant to ¶8-302 a. of the NISPOM, media that contains classified information must be handled in a manner consistent with the handling of classified documents. ¶8-302 b. specifies that all storage media for classified data on dedicated and system high AIS must be labeled and controlled to the highest level of the information on the AIS. Information not at the highest level may be written to appropriately classified/unclassified media using authorized procedures and/or methods. There is no evidence that the media was appropriately marked before it was erased, but where the information was saved to the floppy only for the intent to destroy it, the failure to mark the document was inadvertent.

30. While the incidents in the special access program were not alleged by the Government, the record reflects Applicant committed violations in the special access area as well. Co-workers in the special access program expressed concerns about Applicant's discharge of his security responsibilities.

31. The supervisor's opinion must be evaluated in light of the fact that it had been discovered that he breached his own

security responsibilities in that he failed to report the two incidents involving Applicant's processing of classified information on an unapproved computer.

32. For example, with respect to his processing of the classified table on the unapproved computer system, Applicant testified on direct that co-worker B became suspicious of his actions: "He thought it was a gray area and he told me not to do it." Tr. 2/14/97 p. 114. Co-worker B indicated that he questioned what Applicant was doing and explained to him the auto save function and that "he shouldn't be doing what he was doing on that machine." Tr. 2/14/97 p. 182. The evidence does not reflect that co-worker B was uncertain about the impropriety of Applicant's conduct on that occasion. See also footnotes 11 and 12.

33. As amended, the allegation contains reference to subparagraph 1.e. which was withdrawn by the Government. That pleading defect could easily have been remedied by the Government, but again these are administrative proceedings which require only notice pleading. There is sufficient information in subparagraph 2.a. to place Applicant on notice of the act giving rise to personal conduct concerns.