DATE: November 27, 2006

In re:

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

Applicant for Security Clearance

ISCR Case No. 04-00468

ECISION OF ADMINISTRATIVE JUDGE

ELIZABETH M. MATCHINSKI

APPEARANCES

FOR GOVERNMENT

Braden M. Murphy, Esq., Department Counsel

FOR APPLICANT

William S. Aramony, Esq.

SYNOPSIS

Applicant discovered two confidential COMSEC documents missing from his classified storage container during a routine audit in February 2000. He informed his coworkers, the test site manager, and document control, but did not report the loss to his company's facility security department until May 2003. The security concerns are mitigated since he voluntarily reported the loss, accepted responsibility for his actions, and has positively discharged his security responsibilities for some 25 years. Clearance is granted.

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. As required by Department of Defense Directive 5220.6 ¶ E3.1.2 (Jan. 2, 1960), as amended, DOHA issued a Statement of Reasons (SOR) on March 15, 2005, detailing the basis for its decision-security concerns raised under Guideline K (Security Violations) and Guideline E (Personal Conduct) of the Directive. Applicant answered the SOR in writing on April 26, 2005, and elected to have a hearing before an administrative judge. The case was assigned to me on March 9, 2006, with a motion pending from the government to allege under ¶ 1.a. of Guideline K that Applicant, knowing in February 2000 that two confidential documents assigned to him had been lost, failed to report the losses until May 30, 2003, in violation of ¶ 5-100 of DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM). [(1)] By notice of March 24, 2006, I scheduled a hearing for April 25, 2006.

On April 4, 2006, counsel for Applicant entered his appearance and objected to the motion to amend. He challenged the applicability of the NISPOM to defense contractor employees as well as the legal basis for the proposed amendment. The failure to report the loss, which Applicant admits, was already alleged under Guideline E, and adding the same conduct under Guideline K would unduly prejudice Applicant. I granted the motion to amend on April 5, 2006, as neither the Directive nor Executive Order 10865 precluded the government from alleging conduct under more than one guideline. Applicant's objections to the amendment were taken as a denial of ¶ 1.a, as amended.

With the consent of the parties, I conducted the hearing as scheduled on April 25, 2006, to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. Before the introduction of any evidence, the government moved again to amend SOR ¶ 1.a to indicate that the alleged loss of classified documents would violate ¶ 5-100 and the failure to report ¶ 1-303 of the NISPOM, on the basis the citations to the NISPOM had been inadvertently reversed by the government in its first motion to amend. The motion was granted without any objection from Applicant. Ten government exhibits (Ex. 1-10) and 16 Applicant exhibits (Ex. A-P) were admitted. Sections of the NISPOM, marked for identification as Exhibit 11, were accepted for administrative notice. Applicant and two of his coworkers testified on his behalf, as reflected in a transcript received May 8, 2006.

FINDINGS OF FACT

DOHA alleges that Applicant committed security violations under Guideline K, specifically he violated ¶ 5-100 of the NISPOM in that before February 2000, he lost two documents classified confidential that had been assigned to him, and he violated ¶ 1-303 of the NISPOM in that he knew of the loss in February 2000 and failed to report it until May 30, 2003. The failure to report the loss was also alleged under Guideline E. Applicant admitted two documents marked confidential and assigned to him had been discovered missing in 2000, and while he inquired about the missing documents with several persons, including the building manager and document control person, he failed to report the loss to company security until 2003 but has taken responsibility. He asserted the contractor, who has the reporting responsibility under ¶ 1-303 of the NISPOM, complied with its obligation. After a thorough review of the pleadings, exhibits, and transcript, I make the following findings of fact:

Applicant is a 51-year-old engineering section manager who has been employed by a defense contractor since February 1978. He has held a secret-level clearance throughout his employ, which was last renewed in February 1997. Applicant seeks to retain his secret clearance.

Applicant was briefed annually on his responsibilities for the handling and safeguarding of classified information, including on November 2, 1987, when he executed a classified information nondisclosure agreement certifying he had been briefed. During the majority of his career at the company, he also received communications security (COMSEC) briefings where he was specifically advised it was especially important to the protection of COMSEC information to timely report any compromise or suspected compromise of classified COMSEC information. He executed on September 15, 1982, a briefing certificate attesting to his understanding that the safeguarding of cryptographic information was of the utmost importance, and that its loss or compromise could lead to irreparable damage to the United States.

As of February 2000, Applicant was a principal electrical engineer involved in the integration and testing of a satellite communications system. The work was performed at his employer's communications test site facility, in a temporary building on the grounds of a different facility than where Applicant had his main office. All entrances to the building were secured by lock, with either a receptionist or guard at the entry, and the building was surrounded by a gated, chained linked, barbed wire fence. The perimeter of the entire facility was surrounded by another chain linked, barbed wire fence, with access controlled by guard during the day and protected by roving patrol at night.

Applicant had space in a common area of the communications test site, and as a custodian of classified material, he had primary responsibility for a container authorized to store COMSEC information classified to the secret level. The container was located in a laboratory in a different trailer at the test site than where Applicant worked. The container had four drawers and was secured by an S & G approved locking device that prevented the top drawer from opening without the combination. Once the top drawer was opened, the other drawers were released. Applicant initially shared the container with coworkers X and Y, and then with coworkers X and Z after coworker Y left the company. The classified container was accessed frequently by Applicant and his coworkers X and Y and later X and Z because of the crypto devices and test keys contained therein, although each employee had authorization to access only the documents in his own drawer in the cabinet.

During a routine audit of the classified container in February 2000, Applicant discovered two COMSEC documents classified confidential were missing from his drawer in the container. The documents, signed for by him in May 1994 and December 1995, respectively, and last accessed by him about six months before, had also been regularly used by coworkers X and Y in the past. Since these coworkers already had access to the container, he knew them well, and they

were in a secure facility, Applicant had given them permission to take the documents from his drawer without a hand receipt.

Applicant looked for the documents without success, conducting first a physical search of the general area and places where he usually did business, and then checking with about 30 coworkers. He started with his coworkers who shared the container (coworkers X and Z),[(2)] and within a month expanded his inquiry to others at the test site, including the communications test facility site manager, whom he assumed had onsite security responsibilities because this manager had assisted with security training and was concerned with building security. He also notified document control in person of the results of his audit, including that he had been unable to locate the two confidential COMSEC documents. Document control and the company's security department were located at the facility where Applicant had his main office, and not at the test site. Six months to one year later, he again informed document control that he could not find the documents. Advised by both the test site manager and document control that he should report the loss to the company security manager,[(3)] Applicant responded that since the documents were actively used and shared by several coworkers at the test site, he thought he would find them and would report if the search was unsuccessful. At his hearing, he explained his decision to not go to security at the time:

At the time, I felt that if I kept, I felt I was in a very secure facility, I felt I had, only certain people had access to the area and I felt if I continued to look for them, and eventually someone would, I asked people to do inventories of their own cabinets, keep an eye out for it, I hoped they would show up. (Tr. 108-09)

Over the next three years, Applicant conducted intermittent searches for the documents without success, which consisted of occasionally peaking behind a file cabinet or something like that to see if the documents were there (Tr. 158). Applicant did not conduct a more aggressive search because he was in a secure facility and felt someone would eventually discover them. Applicant was aware as a matter of common sense that he should report the loss or suspected loss of classified information, although he was unaware of any specific time requirement.

The test director of the integration project over the October 1999 to summer 2000 time frame heard second or third hand that Applicant had lost some documents and employees were trying to find them, but he did not investigate as he was not Applicant's direct supervisor. In spring 2001, this supervisor took over as engineering manager for the hardware development group Applicant worked in. Tasked with cleaning up a culture of cutting corners and not performing the work properly, he became impressed by Applicant's level of personal accountability for his work and ability to meet schedule commitments. On his recommendation, Applicant was promoted to section manager (manager III electrical engineering) in 2002.

On January 17, 2002, Applicant was given authorization for access to classified cryptographic information and briefed as to his responsibilities. On April 1, 2002, Applicant was forwarded by internal electronic mail his annual refresher security briefing for the year 2002. In the attached written materials, employees were informed of their obligation to report any suspected loss or compromise of classified information. Applicant performed his duties as test director for a Navy program on schedule and cost, despite taking on a bigger role than planned due to the unavailability of a systems engineer. His overall performance for 2002 was rated as "Exceeds Requirements."

On April 4, 2003, Applicant received a controlled area briefing. With the test site scheduled to move to a new facility in 2003, Applicant realized he was not likely to find the documents and that perhaps company security officials could locate the documents ("I thought security could do a better job, because they have the bigger picture, maybe finding the documents or helping me find them." Tr. 110). In May 2003, Applicant notified company security that two confidential COMSEC documents had been missing since February 9, 2000. At the request of the security manager, Applicant generated a memorandum of ay 28, 2003, detailing the circumstances: he first noticed the confidential COMSEC documents to be missing on February 9, 2000; document control had been notified of the missing documents; all other documents, including those from a second classified shared container in his office had been accounted for; document control was storing all of the classified documents signed out to him pending resolution; and he did not recall lending the missing documents to someone else or forgetting to return them to the classified container. (Ex. 2) Applicant was advised by the security manager that he had committed a very serious violation in failing to timely report within 48 hours the loss of the documents and the Defense Security Service (DSS) would be notified, which was done preliminarily by electronic mail message of June 4, 2003.

Company security conducted its own search for the documents without success. None of the employees who had shared the security container with Applicant in February 2000 were still employed by the company. The originating agency researched the classification status of the missing documents and confirmed both current and historical iterations of the COMSEC documents were still classified confidential, although superceded for technical content.

On June 20, 2003, company security submitted a final report informing the DSS cognizant security office that the two confidential COMSEC documents had been missing since February 2000; that Applicant had notified document control and the "FSO" at the time and indicated he would report the documents as missing if a further search was unsuccessful; that he withheld the information from security hoping the documents would turn up; and that recent security briefings by her office and a concern that his document control privileges could be jeopardized because of the missing documents "prompted him to finally formally report the matter" on May 30, 2003. The DSS was also informed that the company had considered terminating Applicant's employment, but was recommending a five-day unpaid suspension because of mitigating circumstances: Applicant's "reasonably good security" and overall performance record during his 25 years with the company, his willingness to come forward voluntarily and address the issue, and his acceptance of full responsibility. On June 20, 2003, the security manager also submitted an adverse information report to DISCO because of Applicant's recent report that two confidential documents assigned to him had been missing for three years.

Under company disciplinary policies for security violations effective April 8, 2002, disciplinary actions for deliberate or negligent violations ranged from a five-day suspension to employment termination. Because of his "reasonably good security" and overall performance for during his approximate 25 years of employment, his willingness to come forward voluntarily about the incident ("a key consideration"), and his acceptance of responsibility, Applicant was given the minimum. He was suspended from work without pay from July 14, 2003 through July 18, 2003, for his failure to timely report two confidential documents that were identified as missing during an inventory conducted on February 9, 2000. (Ex. A)

On December 5, 2003, Applicant was interviewed by a DSS special agent about the two missing confidential COMSEC documents. Applicant admitted he had noticed them missing in February 2000 but did not formally report it to security because he was hoping they were not lost and he would find them. He added that the documents had been maintained in an approved container he shared with at least two coworkers. The three coworkers (X, Y, and Z) who had access to the container at different times were no longer employed by the company. He informed his coworkers (excepting Mr. Y who had already left the company), the "FSO," and an employee in document control that the documents were missing, but admitted he did not follow up after he failed to locate the documents. He acknowledged he had received annual security briefings and he was wrong to "let this go and not formally report the missing documents to security office as required." With the lab that he worked at being moved, he realized in May 2003 that he needed to finally report the missing documents. Applicant indicated he had "learned his lesson" and would not again fail to report any missing documents. He denied any other security violations and expressed his intent to follow all proper security practices in the future.

In addition to his duties as a section manager, Applicant was an information security lead from spring 2003 through May 2004 on a next generation destroyer technology program. It was a challenging assignment because the system and segment level security requirements were not established until late in 2003. From June 2004 through August 2004, he provided system engineering support to a military satellite communications terminal program, where his major tasks included review of security requirements documentation. Both programs required access to classified material in the performance of his duties, and Applicant received additional security training specific to the program. He showed care in his handling of classified material. In September 2004, Applicant became a hardware development lead for a ground element systems proposal. His overall performance during 2003 and 2004 was rated as "Exceeds Requirements" for both years.

Continuation of Applicant's security clearance has the full support of several longtime coworkers who are aware of the security incident. Applicant's former supervisor from spring 2001 to November 2003, currently director of program management at the company, was present when Applicant was informed of his five-day suspension for failure to report confidential documents were lost. He trusts Applicant. (Tr. 65-66; Ex. H) An engineering fellow at the highest technical level in the company worked with Applicant closely from 2003 to early 2006. He directly observed Applicant to be very conscientious with regard to security, as evidenced in part by Applicant placing a chair across the doorway of his own

office when he was inside as a reminder to not leave the room without first securing his classified container. (Tr. 87) He testified it seemed out of character for Applicant to have made the mistake in judgment in not reporting the loss. (Tr. 88) A system engineer, who has known Applicant since 1984 and served together with him on a system integration team on two satellite communications programs, has always found Applicant to be meticulous about his work and understanding of the importance of security. (Ex. H) Another coworker, who worked with Applicant on a minimum of five projects (three that required access to secret-level information), considers Applicant to be "definitely not a threat to national security and the handling of classified information." (Ex. J)

The company's COMSEC custodian for the facility had previously been assigned to various design and integration programs where he had the opportunity to observe Applicant's handling of sensitive hardware and data on a daily basis, including at the time of the incident. He assisted Applicant in searching for the missing documents, and is unequivocal in his support. (Ex. K) A senior principal engineer with the company nearly 22 years, who has worked with Applicant on a half dozen occasions on a daily basis for several weeks at a time, until recently knew only that Applicant had looked for some missing classified documents a few years ago. After being informed by Applicant of the reasons given for the proposed revocation of his clearance, this coworker considers the loss of Applicant's knowledge and skills could have a greater impact on national security than the "minimal risk associated with allowing [Applicant] to retain his clearance." (Ex. L) Applicant's immediate supervisor for the past three years observed Applicant to be a hardworking and dedicated employee who has been given very demanding assignments. (Ex. N)

Applicant intends to report any violation of which he may become aware to the security manager who "is the best person that would be able to see the big picture." (Tr. 121) He maintains he upheld his responsibility to protect the classified documents, but understands he failed to do the right thing by not filing a timely report with security, which could have provided additional protection to ensure the documents did not get into the wrong hands. (Tr. 122)

POLICIES

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has "the authority to . . . control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position . . . that will give that person access to such information." *Id.* at 527. The President authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960). Each security clearance decision "must be a fair and impartial common sense determination based upon consideration of all the relevant and material information and the pertinent criteria and adjudication policy." Directive ¶ 6.3. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002).

Enclosure 2 of the Directive sets forth personnel security guidelines, as well as the disqualifying conditions (DC) and mitigating conditions (MC) under each guideline. In evaluating the security worthiness of an applicant, the administrative judge must also assess the adjudicative process factors listed in ¶ 6.3 of the Directive. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant. *See* Exec. Or. 10865 § 7. It is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

CONCLUSIONS

Guideline K--Security Violations

Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information. Applicant discovered two confidential COMSEC documents were missing from his classified storage container in February 2000. Since the documents have not been found, they are presumed lost. It was not established that Applicant lost, misplaced, or even inadvertently destroyed the documents. He cannot recall losing them and two appropriately cleared coworkers with access to the container also used the documents in their work. However, he still violated his responsibility under ¶¶ 5-100 of the NISPOM, which requires that individuals safeguard classified information entrusted to them. As the custodian of the documents, he not only had to account for them to

document control, but had to make sure he knew where they were at all times. (Tr. 151) Aware of his responsibility in this regard, he allowed coworkers X and Y to remove the COMSEC documents at issue from his drawer without executing a receipt:

Normally, when you lend a document to someone that has a need to know and has the right clearances, you usually write a hand receipt saying so and so borrowed the document, so I don't forget that I've lent this document out. And they can't keep it for, at the end of the day, they have to, well, actually, they can keep it for longer than a day, but that's the normal process I [sic] usually in place and that's recommended.

Since other people used this constantly, this hand receipt thing was burdensome. I knew the people very well, we were in a secure facility, I gave permission to these individuals to be able to take the document because they had access to the cabinet and to my file drawer, to take the, take it out with the understanding they will protect the documents and inform me if they should go missing or something should go wrong, and that was the understanding we had at the time.

(Tr. 151-52) There is no evidence that such receipts were required rather than recommended by his employer, and the NISPOM requires only external receipt records (*see* ¶ 5-202) when confidential documents are concerned. Yet as a consequence of his failure to maintain such records, Applicant bears sole responsibility for the loss of the confidential COMSEC information. Disqualifying condition (DC) ¶ E2.A11.1.2.2. *Violations that are deliberate or multiple or due to negligence* is implicated. Unauthorized disclosure cannot be ruled out, even though the documents were lost within a secured area, as long as they are still unaccounted for. DC ¶ E2.A11.1.1.2.1. *Unauthorized disclosure of classified information* must also be considered.

The government further alleges that Applicant violated the reporting requirements set forth in ¶ 1-303 of the NISPOM ("Any loss, compromise or suspected compromise of classified information, foreign or domestic, shall be reported to the [Cognizant Security Agency]." Applicant does not deny that he waited until ay 2003 to inform his security manager that the two confidential documents had been missing since February 2000, but he challenges the applicability of ¶1-303 to him on the basis that the reporting requirements apply to the contractors, such as his employer. However, nothing in ¶ 1-303 restricts its application to the contractor. Moreover, under ¶ 1-300 contractors are obligated to establish "such internal procedures as are necessary to ensure that cleared employees are aware of their responsibilities for reporting pertinent information to the FSO, the Federal Bureau of Investigation (FBI), or other Federal authorities as required by this Manual, the terms of a classified contract, and U.S. law." When ¶ 1-300 is read in conjunction with ¶ 1-303.a ("Immediately on receipt of a report of loss, compromise, or suspected compromise of classified information, the contractor shall initiate a preliminary inquiry . . . "), it is clear that employees with clearances have an obligation to report the loss, compromise, or suspected compromise of classified information.

Under ¶ 1-303 of the NISPOM, classified material that cannot be located within a reasonable time is presumed lost until an investigation determines otherwise. Applicant's obligation to report the loss was not immediate, as he would have had a "reasonable period" to search for the documents. I find no violation of the reporting requirement for the first month or so during which he made inquiries of his coworkers, conducted a physical search, and informed both document control and the test site manager of the missing documents. The government did not successfully rebut Applicant's testimony that he was unaware of any requirement to report a loss within 48 hours. However, by his second notification to document control six months to one year later, Applicant had no reasonable excuse for failing to follow both the test site manager's and document control's advice to notify the security department. Even though he thought the test site manager had security responsibilities, he should have questioned that understanding based on the test site manager's advice to notify the security department located away from the test site. The fact that none of his coworkers or document control notified security is troubling, but it does not relieve Applicant of his obligation to report the loss of confidential information. Security concerns are also raised under DC ¶ E2.A11.1.2.2 because of his failure to report the loss over the 2001 to May 2003 time frame.

The loss of the confidential COMSEC material was unintended and limited to a single occurrence. However, mitigating conditions (MC) ¶ E2.A11.1.3.1. *Were inadvertent*, and ¶ E2.A11.1.3.2. *Were isolated or infrequent*, are inapplicable because of his failure to notify security of the loss of the classified material for several years during which time he did little to search for the documents. His security training was deficient in some respects (¶ E2.A11.1.3.3. *Were due to improper or inadequate training*). Applicant was unaware that he was to notify security within 48 hours when he could

not account for classified information. He also appears to have not known that the test site manager had no formal security responsibilities. In its final report to the DSS, the security manager indicates Applicant had notified document control and the "FSO" shortly after he discovered the documents missing. (Ex. 3) Security's identification of the test site manager as the "FSO," which is taken to refer to the test site manager, confirms Applicant was not clear as to the test site manager's responsibilities. An annual security refresher briefing was sent by electronic mail on April 1, 2002, to several cleared employees of the company, including Applicant, which notified them of their reporting responsibilities: " [Company name omitted] employees have an obligation to report events that impact on the status of the facility clearance, personnel clearances or safeguarding classified information. It is especially important to report any suspected loss or compromise of classified information." (Ex. 9) Applicant could not recall reading any particular text on that issue. (Tr. 133) The government did not produce a document certifying Applicant received the briefing and understood his responsibilities, although he testified it was probably very likely that he signed such a document. (Tr. 130) An engineering fellow at the company since 1983 could not attest to whether the annual security briefings at the company included specific advice to promptly report any loss of classified information. Yet both he and Applicant understood it as a matter of common sense in discharging their responsibilities as cleared employees (Tr. 91-92, 117, 127). Having told document control and the test site manager that he would report the loss to security if he had no success in locating the documents, Applicant can reasonably have been expected to follow up with the report. His failure to do so is not attributable to inadequate training, but to a hope that he would find the documents.

As recognized by his employer who imposed the minimum discipline for the violation, Applicant has demonstrated a positive attitude towards the discharge of security responsibilities, which is mitigating under ¶ E2.A11.1.3.4. He had a 24-year record of appropriate handling of classified information before the inadvertent loss of the documents and the reporting violations, marred perhaps only by his admitted dispensation with a recommended security practice of issuing hand receipts to coworkers X and Y who were cleared for access to the information and the security container where they were stored. His self-report of the loss, albeit very belated, is consistent with his fiduciary duty. Since his return following his five-day suspension, he has been given very sensitive duties that require regular access to classified information. He has received additional, very specific security training regarding the protection of COMSEC material. As several coworkers attest, he has handled his responsibilities appropriately and with care over the last three years.

Guideline E--Personal Conduct

Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. Applicant exercised poor judgment within the context of Guideline E by neglecting his fiduciary duty to report the suspected loss of the documents to the security department. The reporting violations, even though not committed with the intent to violate security regulations, increased the risk of the loss or even the unauthorized disclosure of classified information. Although the documents were lost within a secured facility where employees were cleared, not all in the facility had the need to know the specific information. DC ¶ E2.A5.1.2.1. *Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances*, and DC ¶ E2.A5.1.2.5. *A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency*, are implicated.

None of the mitigating conditions apply. While Applicant never lied about the missing documents, and he subsequently notified security without prompting, his ongoing failure to report the loss for over two years precludes the favorable consideration of ¶ E2.A5.1.3.2. *The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily*, or ¶ E2.A5.1.3.3. *The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts*. As credibly argued by Department Counsel, Applicant had opportunities to notify security about the loss when he received his annual security briefing and his COMSEC briefing, yet did not do so until May 2003, but I remain unpersuaded by the government's position that but for the fact that the test site was being moved, Applicant would not have come forward at all. Applicant had informed 30 employees, including the test site manager, that the documents were missing back in 2000. He also told document control twice within the first year.

Whole Person Analysis

As the DOHA Appeal Board held in ISCR 00-0030 (App. Bd. Sep. 20, 2001), "A person who has committed security violations has a very heavy burden of demonstrating that they should be entrusted with classified information. Because security violations strike at the heart of the industrial security program, an Administrative Judge must give any claims of reform and rehabilitation strict scrutiny." Applicant's loss of two classified documents, albeit now technically superceded, and his failure to report it to security after being advised by both the site manager and document control (¶ E2.2.1.1. *The nature, extent, and seriousness of the conduct*), must be evaluated in the context of the "whole person." After a careful weighing of all available information, favorable and unfavorable (¶ E2.2.1), I am persuaded Applicant is likely to act in the best interests of the U.S. and appropriately handle his responsibilities as a cleared employee in the future.

Applicant deserves credit for notifying his coworkers, the site manager, as well as document control, of the missing documents in 2000. Any of these individuals could have filed a report with security and did not do so. The fact that the environment was not neat (Tr. 158) may have led him to believe the documents would eventually turn up. Neither the failure of others to fulfill their reporting obligations nor the physical environment relieves him of his obligation to file a report. Yet had Applicant acted with intent to cover up the loss (¶ E2.2.1.7. *The motivation for the conduct*), he would not have asked for help in searching for the documents. The program technical lead had heard second or third hand that Applicant had lost documents that employees were looking for. (Tr. 70) Applicant has not denied responsibility for the loss of the confidential documents, even though he cannot recall misplacing them, and he now understands that he erred in not reporting the loss to security, which because of access to the "whole picture," can provide additional protection or help locate the documents. (Tr. 121-22) Additional evidence of rehabilitation (¶ E2.2.1.6. *The presence or absence of rehabilitation and other pertinent behavioral changes*) can also be found in his compliance with security requirements on the destroyer technology program since May 2003. An engineering fellow who has worked with him on the program testified to Applicant having put a chair across the doorway when he was in the office with his classified container unlocked as a reminder to not leave the room without securing the container. (Tr. 87) Recurrence is unlikely (¶ E2.2.1.9. *The likelihood of continuation or recurrence*) where he has accepted responsibility and has exhibited good judgment in the handling of classified material for some 25 years.

FORMAL FINDINGS

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

Paragraph 1. Guideline K: FOR APPLICANT

Subparagraph 1.a: For Applicant

Paragraph 2. Guideline E: FOR APPLICANT

Subparagraph 2.a: For Applicant

DECISION

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

Elizabeth M. Matchinski

Administrative Judge

1. The government submitted for administrative notice extracts from the NISPOM dated January 1995. The document was administratively reissued May 2000, changing the paragraph enumeration. In a subsequent reissuance of the NISPOM dated February 28, 2006, the Department of Defense has returned to the numbering of the 1995 version.

2. Applicant indicated he made no inquiry of Mr. Y, who had used the documents in the past but had left the company. (Ex. 5) Mr. X indicated in his letter recommending Applicant (Ex. O) that he had the opportunity to observe Applicant on a daily basis during the time between 1998 and 2003 while they worked on similar programs at the test site. He

indicated he was aware of the matter concerning the security revocation, but denied any personal knowledge of the reasons given in the letter to revoke or the details of the incident. In his sworn statement of December 5, 2003, Applicant indicates he had informed his coworkers, other than Mr. Y, about the missing documents in February 2000 when he began to search for them. Mr. X does not mention that he shared the container nor go into any detail as to what his role might have been, if any, into looking for the documents.

3. Applicant testified to the best of his recollection, it was on his second report to document control that document control recommended he go to security, although he cannot be sure about that. However, the test site manager told Applicant to report the matter to security within a month or two of when he discovered the documents were missing. (Tr. 141-42)