KEYWORD: Security Violations

DIGEST: Applicant is a computer systems administrator who failed to properly secure a classified storage container in September 1997, September 1999, February 2001, July 2002, and November 2002. He failed to safeguard two classified hard disk drives in his custody, and one disk was still unaccounted for as of March 2007. In August 2006, he left a TOP SECRET tape cartridge unprotected on top of a classified storage container, failing to secure it before he left the office. His multiple security violations, while unintentional, raise considerable doubts about his ability to meet his security clearance obligations. Clearance is denied.

CASENO: 05-01305.h1

DATE: 05/07/2007

DATE: May 7, 2007

In re:	)	
	)	
----------	)	ISCR Case No. 05-01305
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

DECISION OF ADMINISTRATIVE JUDGE
ELIZABETH M. MATCHINSKI

APPEARANCES

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

FOR APPLICANT
Nicolas A. Gordon, Esq.

SYNOPSIS

Applicant is a computer systems administrator who failed to properly secure a classified storage container in September 1997, September 1999, February 2001, July 2002, and November 2002. He failed to safeguard two classified hard disk drives in his custody, and one disk was still unaccounted for as of March 2007. In August 2006, he left a TOP SECRET tape cartridge unprotected on top of a classified storage container, failing to secure it before he left the office. His multiple security violations, while unintentional, raise considerable doubts about his ability to meet his security clearance obligations. Clearance is denied.

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. As required by Department of Defense Directive 5220.6 ¶ E3.1.2 (Jan. 2, 1992), as amended, DOHA issued a Statement of Reasons (SOR) on August 26, 2005, detailing the basis for its decision–security concerns raised under Guideline K (Security Violations) of the adjudicative guidelines. Applicant answered the SOR on October 12, 2006, and elected to have a hearing before an administrative judge. The case was assigned to me on November 30, 2006. On January 25, 2007, I scheduled a hearing for March 1, 2007.

On January 29, 2007, the government moved to amend the SOR to add ¶ 1.h under Guideline K, alleging that on or about August 18, 2006, Applicant failed to properly secure a box that held a tape cartridge marked TOP SECRET and an envelope marked TOP SECRET that contained classified password information, thereby violating ¶¶ 5-100 and 5-303 of the National Industrial Security Program Operating Manual (NISPOM) issued January 1995[1] as well as ¶¶ 4.7, 4.15, and 4.16 of Section 12 and ¶ 3.1 of Section 17 of his employer's standards practices procedures (SPP). On January 30, 2007, I granted the motion and gave Applicant until February 20, 2007, to respond to ¶ 1.h or it would be considered admitted.

In a conference call with the parties on February 28, 2007, Applicant requested a continuance and indicated he had no objection to ¶ 1.h as proposed. The SOR was accordingly amended as requested by the government. Applicant was also granted a brief continuance.

A hearing was convened on March 29, 2007, to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The government's case consisted of 29 exhibits (Ex. 1- 29), entered without objection, and the testimony of a Defense Security Service (DSS) senior industrial security specialist. Applicant submitted 11 exhibits (Ex. A-J, and L) into the record. An additional document, initially identified as Ex. K, was withdrawn. Applicant and his supervisor testified, as reflected in a hearing transcript (Tr.) received on April 12, 2007.

[1]The NISPOM, DoD 5220.22-M, was reissued on February 28, 2006. On the reissuance, the January 1995 NISPOM was cancelled. It was therefore error for the government to allege a violation of the January 1995 NISPOM in August 2006, although ¶ 5-100 (the obligation to safeguard classified information) had not changed.

FINDINGS OF FACT

In the SOR as amended, DOHA alleges Applicant failed to properly secure a DoD approved security container on September 14, 1997 (SOR ¶ 1.a), September 11, 1999 (SOR ¶ 1.b), February 28, 2001 (¶ 1.c), July 25, 2002 (¶ 1.e), and November 24, 2002 (¶ 1.f), Applicant is also alleged to have failed to properly secure a classified computer hard disk drive in about 2002 (¶ 1.d) and in April 2003 (¶ 1.g), and a box containing TOP SECRET information on or about August 18, 2006 (¶1.h). The conduct set forth in SOR ¶¶ 1.a through 1.h was alleged to be in violation of ¶¶ 5-100 and 5-303 of the NISPOM, and Section 12 ¶¶ 4.7, 4.15, and 4.16 and Section 17 ¶ 3.1 of his employer's SPP.

Applicant admits he failed to secure the approved security container on the dates alleged, but offers in mitigation that he had access less than 30 days (September 1997); had additional responsibilities (September 1999 and February 2001); the computer hard drive had been transferred to him and been removed from service for two years and was not used to store classified data (2002); no compromise of classified information occurred as confirmed by full inventory (September 1997, September 1999, February 2001, July 2002, November 2002); the hard drive not secured in April 2003 was found installed in an existing classified system as a secondary drive in a secure environment; and the recent violation was an oversight. He averred all of the incidents occurred in a closed area with access limited to those with SECRET-level clearances and "need-to-know," and that as a result of the April 2003 incident concerning the system hard drive, new security procedures had been implemented at the company.

After consideration of the pleadings, exhibits, and hearing transcript, I make the following findings of fact:

Applicant is a 39-year-old senior systems administrator who has worked for a defense contractor since July 1997, staying on with the company after it was purchased by another defense firm in 1999. Applicant was initially granted a SECRET-level security clearance for his duties as a computer software analyst in the Army National Guard. That clearance was transferred on his employ with the defense contractor. His clearance was subsequently upgraded to TOP SECRET in October 1998.

In August 1997, Applicant was granted a SECRET-level clearance for his duties as systems administrator for a UNIX-based classified engineering platform supporting various encryption products developed by the company for multiple U.S. government contracts. He was assigned responsibility for a classified container approved for the storage of SECRET/COMSEC (communications security) information and briefed as to his COMSEC responsibilities.[2] The storage container was located in a Department of Defense–accredited closed area of the facility where access was limited to those cleared to the SECRET level at a minimum and had a "need to know."[3]

[2]Applicant testified, unrebutted by the government, that he was briefed by document as to his COMSEC responsibilities. (Tr. 135)

[3]Personnel access to the facility was and continues to be controlled by a professional proprietary guard force that conducts foot patrols and monitors a central control station equipped with a closed circuit television system and a DoD-accredited alarm/card access control system. The closed area and building perimeter are equipped with a card reader system unique to the facility. In addition, the closed area entrance is equipped with a closed circuit camera for monitoring purposes. (*See* Ex. 22)

Applicant regularly accessed the storage container in performing his duties, which included not only configuring and maintaining the UNIX workstations and servers, but also maintaining backup tapes that were stored in the container. On September 14, 1997, he failed to properly secure the security container (SOR ¶ 1.a) due to oversight. (Ex. 14) An inventory of the storage container was conducted and all classified materials were accounted for. Applicant was counseled about this security lapse, which he attributed to his lack of experience and failure to appreciate the importance of security.

Applicant demonstrated core competencies during his first full year on the job. Well liked by the project users, and technically proficient, Applicant looked for ways to become more efficient. Not one to be intimidated by new problems, Applicant was noted by his supervisor as sometimes taking on "sometimes too many" new challenges. (Ex. C)

In 1999, Applicant's employer was acquired by a large defense contracting firm. Applicant was promoted to the position of lead system administrator, and was responsible for providing administrative support for a large classified local area network with more than 150 workstations. On September 10, 1999, Applicant accessed a security container approved to safeguard SECRET/COMSEC material. His supervisor was the primary custodian for the container, which was located in a DoD–accredited closed area. Applicant was the alternate custodian. Applicant got distracted by employees needing his systems administration assistance, and he failed to properly secure the container before he left the facility at around 1630 hours. (SOR ¶ 1.b) At around 0100 hours the next morning, a cleared member of the plant protection staff discovered the container unsecured and unattended. He noted a random sample of the contents and secured the container. Company security conducted an administrative inquiry during which the classified material assigned to all custodians of record was inventoried. All material was properly accounted for. The combination to the security container was also changed. Applicant was found responsible for a non-deliberate security violation and his supervisor was informed. On September 17, 1999, Applicant's employer notified the government agency with cognizance over the classified material (government agency X) of Applicant's culpability and of its conclusion that no loss or compromise had occurred. (Ex. 22)

On February 28, 2001, Applicant failed to properly secure his security container approved to safeguard SECRET/COMSEC classified material when he left the facility for the day at around 1650 hours. Involved at the time in restoring computer files to the system, Applicant again got distracted by activity in the closed area and system user inquiries. (SOR ¶ 1.c) A plant protection guard discovered the container unsecured at around 1720. As in 1999, the company performed an inventory of all classified material assigned to Applicant as custodian of the container, and all classified material was properly accounted for. The classified material involved in this incident was not accountable under the COMSEC account. On March 14, 2001, company security notified government agency X of its findings that Applicant was culpable, but that no loss or compromise had occurred. Applicant was re-indoctrinated as to his security responsibilities. (Ex. 21) Because the incident did not involve any COMSEC material, government agency X considered it "Not a Reportable Incident" but informed the company that it had to be reported to the local Defense Security Service (DSS) industrial security representative. (Ex. 20)

On February 20, 2001, Applicant was assigned custodial responsibility for a SECRET/COMSEC hard disk drive that had been in the company's classified document accountability system since February 27, 1995. The disk drive was transferred to Applicant when the

former custodian left the company. In March 2001, a cleared member of the security department conducted a classified material inventory of Applicant's holdings and personally sighted the hard disk drive. The hard disk drive was integral to a workstation that was installed only with a specific UNIX operating system. The client/server configuration for the system was such that all user data was stored on the server rather than on the workstation's disk. The workstation was used only as a display device and for its processing power. On or about August 14, 2001, the workstation associated with the hard disk drive was sent to recycling to be crushed. Before the workstation was released from the classified environment, it was checked by a cleared member of the engineering staff to ensure that the hard disk drive had been removed. (Exs. 9, 10, 16)

During internal security reviews conducted from March 2002 and May 2002, the hard disk drive could not be located. The company's classified material control center operations were reviewed, including all custodian security files, and accountability and transaction records. When questioned about the hard disk drive, Applicant expressed his belief that the disk drive had been returned to the classified material control center on July 10, 2001, for destruction along with other classified hard drives, but the classified material control center's database and signature cards revealed Applicant was still the active custodian. Applicant was assessed as culpable for the loss of the hard disk drive as he was the custodian of record (SOR ¶ 1.d), and the company submitted an adverse information report to DISCO. Applicant was also re-briefed as to his responsibilities. (Ex. 10) As a direct result of the incident, systems administrators were required to audit each other six months before the annual security department audit due to the large volume of classified assets assigned to them. Two person validation was also required for any changes to classified inventory, *i.e.*, items to be disposed of as surplus, turned in for destruction, brought into accountability. (Ex. 16) Markings were to be affixed to the media inside a workstation when the media was removed and security numbers of the drive placed in the title of the document so that any media to be destroyed could be tracked by both the document control number and the serial number.

On July 25, 2002, Applicant failed to properly secure his security container approved to safeguard SECRET/COMSEC classified material when he left the facility for the day at around 1700 hours. Applicant again got distracted by activity in the closed area and system user inquiries. (SOR ¶ 1.e) A plant protection guard discovered the container unsecured at around 1815, and conducted a random sample of the contents, which were not accountable under the COMSEC account. An inventory was conducted and all classified material properly accounted for. On September 12, 2002, company security notified government agency X of the violation, its conclusion that no loss or compromise had occurred, and that Applicant had been re-indoctrinated as to his security responsibilities. (Ex. 19) Government agency X considered the occurrence as a practice dangerous to security. (Ex. 18)

On November 7, 2002, company security notified government agency X it had been unable to locate a hard drive missing since the inventory of Applicant's container conducted between March and May 2002 (¶ 1.d). While compromise was possible, company security personnel considered it very low or remote given the system configuration (classified information was processed using the workstation to a server environment and not to the operating system's hard disk drive). The company speculated that the disk drive may have been removed from the personal computer tower and inadvertently turned in to the classified material control center absent any control number or security classification marking, since in the early 1990s the company had affixed the classified material control numbers to the personal computer tower and not the hard drive disk itself. The item would

have been treated as "company sensitive" and destroyed in the same manner as classified material was destroyed under the contract. (Ex. 16) Government agency X did not conduct an independent evaluation since there was no COMSEC involved. (Ex. 15) The DSS subsequently filed its own report of the loss to government agency X. While the DSS agreed that the hard disk drive likely was shipped to the government contracting agency and destroyed in the same manner as material that bore classified markings, there was no guarantee that the hard disk drive had been destroyed. There was no record that the hard disk drive had been shipped to the government. Since the hard drive had not been located, it was considered a loss by the DSS. (Ex. 10)

Applicant left his security container unsecured on November 24, 2002 (¶ 1.f). He had come in to work on a Sunday to correct problems on the servers, and short on time, neglected to lock the classified storage container before he left at around 1545 hours. A plant protection officer discovered the violation at around 1725 hours. (Ex. 11) An inventory of the container revealed no loss of any accountable items. In reporting the incident to company security, Applicant's supervisor noted the rigors and hectic activity in the laboratory where the container was located and Applicant being usually the first "to bring to peoples [sic] attention concerns and policies related to security." In an effort to prevent a recurrence, the supervisor recommended to Applicant that he put the lock for the container in his pocket. The container was also removed from the server area to force Applicant to leave his workstation to obtain classified material. The hope was that it would eliminate the possibility of Applicant leaving the container open when he was working. Steps were also taken to eliminate the old backup tapes stored in Applicant's container as they were no longer needed. Applicant was informed that another security violation within the calender year would result in a reprimand and a week off without pay. (Ex. 14) Company security concluded there was no loss or compromise of classified material, but filed an adverse information report with the Defense Security Service Operations Center on January 10, 2003, since it was Applicant's third security violation in a calendar year. (Ex. 12, Ex. 13) Government agency X evaluated the occurrence as a "Practice Dangerous to Security." (Ex. 11)

On June 25, 2003, Applicant was interviewed by a DSS special agent about his security violations. He acknowledged he had failed to properly secure his classified storage container in September 1997, September 1999, February 2001, July 2002, and November 2002, but asserted he had not had a similar security lapse since his storage container had been moved from his immediate work area. As for the missing hard drive, Applicant explained that the disk lost since 2001 had been in a system processed for surplus, but that particular hard drive disk had not been recorded as having been returned to the classified material control center. He indicated it might have been left in the computer, the contents of which were not checked before disposal. Since the hard drive was configured to operate the system and not to store information, Applicant maintained there could not have been any classified information on the missing hard drive. Applicant also indicated that security was investigating the loss of a second hard disk drive that could not be located during an audit of his classified storage container in April 2003. He could not recall what happened to the disk after he validated that the disk was defective in September 2002, but asserted it did not contain classified material.

In August 2003, company security notified the DSS that it could not account for a second hard disk drive (¶ 1.g). The hard disk drive, internal to an unclassified workstation, had been brought into company classified material control accountability on July 30, 2002, when the workstation was connected to an approved information system classified SECRET/COMSEC. After installation of

the operating system failed, the engineer with custody returned the hard disk drive to the classified material control center for destruction. On September 9, 2002, Applicant had taken custody of the hard disk drive from the classified material control center after a series of internal disk drive failures. As systems administrator for the SECRET/COMSEC information system, he wanted to determine the cause of the disk failure. An internal review of all classified material assigned to the facility was conducted between March 2003 and June 11, 2003. During the course of this audit, the hard disk drive could not be found. The classified material control center's operations, including all custodian security files at the facility, were then re-inventoried, all accountability and transaction records were examined, and every controlled system tower under the SECRET/COMSEC information system was opened with drives verified by inventory records. When the hard disk drive failed to turn up after all these reviews, Applicant was assessed culpability for failure to account for the hard drive and he was suspended for one week without pay from work effective August 11, 2003. He was also briefed on security awareness, but the company did not consider removing him from his position of information systems security officer. A new department policy was instituted prohibiting the recall of any controlled item turned in to the classified material control center for destruction. Another employee was also hired to take over part of Applicant's demanding workload. Company security concluded that a loss had occurred but that the possibility of a compromise of classified information did not appear to exist as the disk drive was in a defective state (could not initiate installation of the operating system) when it left the classified material control center. Per Applicant, who was the systems administrator, further testing would not have exposed the hard disk drive to classified information. (Ex. 7; Ex. 8)

On November 26, 2003, the DSS notified government agency X that the hard disk drive could not be located and must be considered lost. Compromise could not be ruled out since it was not known what information was transferred, if any, to the hard drive during the failed installation, and Applicant was unable to recall what he did with the hard disk drive after he took custody. It could have been connected to the system after the failed installation as it bore classified markings and anyone finding it would assume it could be used on a classified system. (Ex. 5; Ex. 6) On December 1, 2003, the DSS issued an adverse information report noting Applicant's culpability for failure to account for the hard disk drive, which had to be treated as SECRET/COMSEC, due to its connection to a classified network and unavailability for review.[4] (Ex. 4) In about June 2004, a subordinate of Applicant's discovered the hard disk drive installed in an existing classified system as a secondary drive connected via data and power cables but not configured for access by the classified system. Subsequent checks of the internal hard disk drive verified that the disk had no interaction with the classified network. The disk had not been modified after the operating system installation failed. (Ex. L) [5]

[4]A DSS industrial security representative with cognizance over the facility until 2004 testified that since the hard drive was unavailable for review, DSS could not determine for certain that no classified was on the drive. It had been connected to a classified system so it was possible that classified information was on the disk and had to be treated as such. (Tr. 84-86)

[5]Applicant reaffirmed at his hearing that the drive could not have been used. Unable to recall previously, he claimed to have a clear recollection of having installed it into the system where it was found ("it was the way it was installed, I knew it was mine. Those systems are not opened without our permission or without our direct involvement. . ." Tr. 237).

On August 26, 2005, DOHA issued an SOR to Applicant because of his failures to properly secure DoD approved security containers in September 1997, September 1999, February 2001, July 2002, and November 2002, and failures to properly secure classified computer hard disk drives in 2002 and in April 2003. Applicant admitted the violations but indicated that he had made significant changes in his work procedures as evidenced by the absence of any security violations and 100% audit of his classified holdings for the past two years.

At around 1630 hours on August 18, 2006, Applicant accessed a classified storage container in the security office to transfer backup media. Applicant was supporting another systems administrator at the time and not entirely familiar with the routine. He removed a cardboard box containing a tape cartridge marked TOP SECRET in order to access the needed classified tapes under it. Also in the box was a white envelope containing password information marked TOP SECRET. After he completed the transfer of tapes, he secured the cabinet leaving the box containing the password information and classified tape cartridge unsecured on top of the container. (Ex. 24; Ex. 26) At about 1745 hours, the plant protection supervisor noticed the TOP SECRET material and properly secured it. (Ex. 24; Ex. 25) Company security personnel conducted an administrative inquiry into the violation. In reporting the violation to the DSS in January 2007, the security manager indicated that the envelope marked TOP SECRET actually contained unclassified interim passwords used to initialize a server prior to the server being deployed in a classified environment, and that it was a common practice by the engineering organization to record passwords on the server while it was being built to ensure they were not forgotten. Once deployed in the classified environment, the passwords were changed and the server brought into accountability. The security manager also maintained that there had been no compromise of the tape cartridge that was classified, as the security office, although not located in a closed area, had been occupied until 1730 hours when the last person left and locked the door. Anyone that would have entered the office during non-working hours would have been challenged by security office personnel. In addition, the classified information on the cartridge could be accessed only through a compatible classified information system. Applicant's supervisor was notified of the violation, but since it was Applicant's first in a 12-month period, disciplinary action was not warranted under company security policy. (Ex. 24)

Applicant has consistently exceeded position expectations in a demanding classified environment. (Ex. A–Ex. J) As an information systems security officer for the past five or so years as well as the senior systems administrator for two particular classified systems, he has supported the information systems security manager who has overall responsibility for information security policy and implementation at the facility. In 2003, Applicant struggled in some areas including implementation of automated information systems security requirements, due to the high workload, a coworker's failure to meet work expectations, and Applicant's efforts to keep systems users happy. (Ex. G) He worked diligently to bring the systems into compliance with the NISPOM in 2004. (Ex. H) Due in large part to Applicant's dedication, NISPOM requirements were met on a daily basis, and Applicant met his goal of no security violations in 2005 (Ex. I). Noting that Applicant faced potential loss of his clearance due to past security violations, Applicant's manager noted in his evaluation of Applicant's performance for 2005 that the loss of clearance by Applicant would have a major impact in support of the classified systems. (Ex. I)

In 2006, Applicant continued to manage the software development engineering for classified projects in his building, to configure and maintain UNIX workstations and servers, to provide support for users, to interface with vendors, to support program management, and to train and mentor

the coworker hired to take on some of his responsibilities.(Ex. J) Applicant's continued access to classified material is supported by his supervisor, the information systems security manager, and another systems administrator. Applicant has a reputation at work of requiring the users of his systems to comply with security requirements. The company's information systems security manager attributes Applicant's violations to Applicant's desire to take full responsibility for the environment and to maintain control over all assets rather than delegate to others. In his opinion, none of Applicant's violations were intentional or due to reckless disregard of security procedures, and the potential for future security incidents has been reduced by the implementation of procedures designed to give Applicant more time and attention to the protection of classified assets. (Ex. A) A systems administrator attests to Applicant demonstrating technical excellence as well as insistence on strict adherence to security guidelines by team members. He has experienced Applicant as "zealous in educating himself in proper handling procedures and rules and then in disseminating this information to members of the team." (Ex. B) As of 2007, Applicant was responsible for between 130-150 classified assets (systems as well as tapes stored on a regular basis), as half of his work had been delegated to a capable subordinate.

POLICIES

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

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

CONCLUSIONS

Guideline K—Security Violations

Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information. Directive ¶ E2.A11.1.1 Responsible under the NISPOM and his employer's security policy (SPP) to safeguard classified information under his custody or in his control, Applicant violated NISPOM ¶ 5-100 and his company's SPP §

12 ¶¶ 3.1, 4.7, 4.15, 4.16[6] on several occasions between 1997 and August 2006. On five separate occasions between September 1997 and November 2002, he failed to properly secure a container approved for the storage of information classified to the SECRET-level. Sometime after March 2001, he could not account for a hard disk drive classified SECRET/COMSEC for which he was the custodian of record. As of March 2007, that disk drive had not been located. A second hard disk drive that Applicant took custody of in September 2001 was missing until about June 2004 when it was discovered as a secondary drive in a computer system. Since the hard disk drive had been in a workstation connected to a classified system and used in a failed effort to upload a classified operating system, it was required to be protected as SECRET until it could be cleaned or at least verified to be defective. In failing to properly safeguard the classified hard drive, he violated the security procedures in place to protect automated information system media set forth in ¶¶ 8-105.c(1) and 8-105.c(3), and because of his position as information systems security officer, NISPOM ¶ 8-104 as well.[7] More recently in August 2006, he left a TOP SECRET tape cartridge out in the open in the security office. Unlike in the earlier security incidents, the security office was not located in a closed area of the facility. Since he left TOP SECRET information vulnerable to compromise, Applicant violated ¶ 5-302 of the NISPOM, dated February 28, 2006, and § 17 ¶ 3.1 of his employer's security policies,[8] in addition to NISPOM ¶ 5-100 and § 12 ¶¶ 3.1, 4.7, 4.15, 4.16 of the company's SPP. Guideline K disqualifying condition ¶ E2.A11.1.2.2, *violations that are deliberate or multiple or due to negligence*, is implicated by his record of eight separate security infractions over a ten-year span.

Two of Guideline K's four mitigating conditions are potentially applicable. ¶ E2.A11.1.3.2, *violations that were isolated or infrequent,* cannot reasonably be considered, even though his eight infractions represent a very small percentage in terms of opportunity. Individuals with security oversight responsibilities must be counted on to fulfill their obligation to safeguard classified material at all times. Improper or inadequate security training (*see* ¶ E2.A11.1.3.3) was not the cause of Applicant's leaving his security container unsecured. Even if his initial briefing was not to the detail that Applicant would have liked, he knew he had to lock his classified storage container when it was not in use. However, since none of the violations was deliberate, ¶ E2.A11.1.3.1, *violations that were inadvertent*, must be considered. Furthermore, Applicant's supervisor and the information

[6]NISPOM ¶ 5-100 sets forth the general requirement for contractors and individuals to safeguard the classified information in their custody and/or control. Company security policy provides under §12 ¶ 3.1 that all employees, contract labor personnel and consultants are responsible for providing the proper protection and accountability for all classified information entrusted to them at all times. § 12 ¶ 4.7 requires employees to safeguard all classified information under their control and to adhere to the security policy and procedures to preclude the possibility of access to classified information by unauthorized persons. § 12 ¶ 4.15 mandates compliance with established procedures in the protection, recording, and storage of classified material issued to them for their use. § 12 ¶ 4.16 mandates employees control classified material entrusted to them.

[7]Under ¶ 8-105.c.(1) all users are required to comply with the industrial security program requirements. ¶ 8-105.c(3) specifies that all users are accountable for their actions on an information security system. Under ¶ 8-104.a. information system security officers are required to ensure the implementation of security measures, in accordance with facility procedures. These include implementation of the facility procedures governing the marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information (¶ 8-104.i.(1).

[8]NISPOM ¶ 5-302 requires that TOP SECRET material shall be stored in a GSA-approved security container, an approved vault, or an approved closed area with supplemental controls). The company's security policy specifies under § 17 ¶ 3.1 of its manual (Ex. 3) that all TOP SECRET, SECRET, and CONFIDENTIAL material shall be stored in an approved security container, vault or Closed Area when not in use.

systems security manager attest to Applicant's efforts to ensure that the users of his classified systems comply with their security obligations, and to Applicant's collaboration in formulating corrective actions to avoid recurrence, such as carrying the lock in his pocket and relocating the security container outside of his immediate work area. These reflect a positive attitude by Applicant toward the discharge of his security responsibilities (*see* ¶ E2.A11.1.3.4). Yet, changes instituted to prevent a recurrence, most notably reducing by about half the number of classified assets within his security cognizance, did not preclude him from again becoming distracted and leaving a TOP SECRET tape cartridge out and unprotected on top of a security cabinet in August 2006. Fortuitously for Applicant, compromise was unlikely in that incident, given the information on the TOP SECRET cartridge could not be easily accessed without the proper software, and the office was locked during the 15 minutes it was exposed with no security personnel in the office. While Applicant's willingness to comply with his security obligations is unquestioned, this recent security violation raises substantial doubts about his ability to comply.

"The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance." Directive ¶ E2.2.1. Applicant's overwhelming workload, especially when he had responsibility for some 275 classified assets, is a factor that contributed to his violations, especially his failures to secure classified storage containers in 2001 and 2002 (*see* ¶ E2.2.1.2. *The circumstances surrounding the conduct, to include knowledgeable participation*). However, Applicant's record of violations also spans most of his employment with the defense contractor. Only two months into his job, he failed to lock a security container. His latest violation comes after nine years of experience in security, including about five years as an information systems security officer, one year after the SOR was issued, and despite his goal of no future security violations (*see* ¶ E2.2.1.1. *The nature, extent, and seriousness of the conduct*; ¶ E2.2.1.3. *The frequency and recency of the conduct*). Steps taken by his employer (moving his classified storage container, reducing his classified holdings, prohibiting recall of items turned in to classified material control), have not proven to be successful in dealing with the root cause of the violations (*see* ¶ E2.2.1.6. *The presence or absence of rehabilitation and other pertinent behavioral changes*). With Applicant still vulnerable to workplace distractions,[9] another security incident cannot be ruled out (*see* ¶ E2.2.1.9. *The likelihood of continuation or recurrence*).

FORMAL FINDINGS

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

Paragraph 1. Guideline K:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	Against Applicant

[9]Concerning the August 2006 infraction, Applicant testified that as he was starting the process of swapping out the tapes from the classified storage container, the director of security came out and asked him what was up ("You know, because he heard me, and you know, a bit of a start, I stopped, hey, how are you, just doing tapes, blah, blah, blah and, at that point continue on my work. Again, secured the container, completed my log, validated the lock and I left the office." Tr. 248).

Subparagraph 1.d:	Against Applicant
Subparagraph 1.e:	Against Applicant
Subparagraph 1.f:	Against Applicant
Subparagraph 1.g:	Against Applicant
Subparagraph 1.h:	Against Applicant

DECISION

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

Elizabeth M. Matchinski
Administrative Judge