DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 07-18613
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Gina L. Marine, Esquire, Department Counsel
For Applicant: *Pro se*

April 28, 2010

Decision

MATCHINSKI, Elizabeth M., Administrative Judge:

During the 2004/05 time frame, Applicant failed to protect classified and special access program information while employed as a security manager for a defense contractor. She knowingly failed to maintain proper accountability of some top-secret classified documents, and exposed classified and special access restricted information to possible compromise by storing it in a vault accessed by employees not briefed to the program. Data was placed on a local area network (LAN) within her security cognizance in violation of a co-utilization agreement and the system's protection level. The evidence of reform is insufficient to overcome the serious concerns regarding the handling of protected information. But personal conduct concerns are not established in the absence of proof that Applicant acted with the intent to conceal or withhold classified material from government inspectors. Clearance is denied.

Statement of the Case

Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) on January 27, 2004. On October 24, 2008, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant detailing the

security concerns under Guideline K, handling protected information, and Guideline E, personal conduct, that provided the basis for its preliminary decision to deny her a security clearance. The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) promulgated by the President on December 29, 2005, and effective within the Department of Defense as of September 1, 2006.

Applicant responded to the SOR on November 13, 2008, and she requested a hearing. On July 28, 2009, the case was assigned to me to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. On September 1, 2009, I scheduled a hearing for October 27, 2009.

I convened the hearing as scheduled. Ten Government exhibits (Ex. 1-10) were offered into evidence. Exhibits 9 and 10 consisted of four separate documents that were marked as Ex. 9.a-9.d and 10.a-10.d for ease of reference. Applicant did not object to Exhibits 1, 2, 8, 9.a, 9.c, 9.d, 10.a, and 10.c, and those documents were admitted. Exhibits 3, 4, 5, 6, 7, and 9.b were accepted into the record over Applicant's objections.[1] Applicant also objected to the inclusion of those documents marked as Ex. 10.b and 10.d. The Government withdrew those documents. Applicant offered nine exhibits (Ex. A-I) that were admitted without objection, and she testified, as reflected in a transcript (Tr.) received on November 4, 2009.

Findings of Fact

DOHA alleged under Guideline K, handling protected information, that the military found Applicant responsible for two security violations following an inspection of a sensitive compartmented information facility (SCIF) around October 2004 (SOR 1.a); that Applicant's special access privileges were suspended by her employer (SOR 1.b) and by a U.S. military special access program security office (MSAPSO) (SOR 1.c) in January 2005 pending an investigation into noncompliance with a co-utilization agreement involving special access programs (SAPs) at Applicant's facility; and that the MSAPSO office found Applicant culpable in April 2005 of: (1) direct involvement in the mishandling of top secret/special access program (TS/SAP) materials, (2) contributing to the unauthorized exposure of classified special access material to "non-accessed" (unauthorized) individuals, (3) knowingly violating established co-utilization agreements

[1]Applicant objected to exhibits 3, 4, 7, and 9.b on the basis that the signatory for the MSAPSO was a contractor and not authorized to act on behalf of the military security office. Applicant was offered an opportunity to present evidence after her hearing to support her contention, but at the close of her case, she elected not to request to leave the record open because she did not believe the government would provide her with the information. She objected to Exhibit 5 to the extent that it contained opinions of the investigator. Her concerns were noted in evaluating the weight to be afforded the information in the document. Applicant objected to exhibit 6, a report of inquiry conducted by the MSAPSO, on the basis that information had been redacted from the document. Since the redaction was only of program/LAN identifying information that would have been within the knowledge of the Applicant, I accepted the MSAPSO report into evidence. The cognizant security agency has an obligation to ascertain whether classified information is adequately protected.

by using an unauthorized local area network (LAN), and (4) willfully withholding classified material from cognizant security authority (CSA) inspection or oversight or both (SOR 1.d). DOHA alleged that as a result of those findings, the MSAPSO recommended in June 2005 that her access to special access programs be revoked (SOR 1.e). The willful withholding of classified material from the CSA was cross-alleged under Guideline E (SOR 2.a).

In her Answer, Applicant denied that she was issued a security violation as a result of the inspection conducted of the SCIF in October 2004 (SOR 1.a). Concerning the alleged violation of the co-utilization agreement (SOR 1.b and 1.c), Applicant admitted the actions taken by her employer and the U.S. military to suspend her access, but she denied any authority over the LAN involved. Applicant denied she mishandled TS/SAP materials (SOR 1.d). Applicant asserted that once she discovered that TS/SAP material was not in proper accountability, she made every effort to bring it under proper controls and to notify the SAP's security officials. She took steps to ensure that unauthorized personnel were not exposed to SAP information by separating combination logs, and physically moving material to a locked area. She also denied any willful withholding of classified material from CSA oversight (SOR 1.d(4) and 2.a), inasmuch as she was the first security manager to list all areas, including that which housed the SAP material, on the inspection report submitted to the inspection team before its arrival.

After considering the pleadings, exhibits, and transcript, I make the following findings of fact.

Applicant is a 46-year-old employee of a defense contractor. She has been employed in the engineering department as a configuration management specialist since June 2005. (Ex. 2) She started working for her employer in October 1984, initially as an inspector in final assembly involving a military SAP (hereafter SAP X). She moved to another program as an inspector, where she worked until May 1988, when she became a security aide in the special security office (SAPSO) under the supervision of a security manager (hereafter security manager A). (Ex. 1, I, Tr. 120-21.) In August 1995, Applicant left the company. She returned to work for the defense contractor in February 1999 in the position of security aide involved in automated information systems (AIS). (Ex. 1, 2, 5.) Around August 1999, Applicant was granted a TS security clearance for her duties. (Ex. 9.b.)

Applicant lacked the technical expertise to perform the AIS security duties required, so in about January 2000, she went back to the SAPSO where she performed administrative work at a junior level. (Ex. 2, Tr. 89, 125-26.) In March 2000, Applicant was briefed into SAP X. She initially split her time between that SAP program and information technology security for a different program. Applicant learned about security on the job, and was given no formal security training. She was provided an automated information security account, and her duties involved correcting deficiencies and maintaining receipt and dispatch records. (Ex. 5) Applicant worked under security manager A, who was the Contractor Program Security Officer (CPSO) for SAP X. (Tr.

124-26.) In October 2001, Applicant was cleared for access to sensitive compartmented information (SCI). (Ex. 1.)

During a 2002 government security review of SAP X at the facility, TS accountability was determined to be insufficient, and that all TS program material needed to be accounted for by the CPSO. In April 2002, Applicant was promoted to a security representative position, which meant for her a loss of overtime pay, and in May 2002, she was designated as CPSO for SAP X. Her manager transitioned out of the office and became the manager of special programs security (Ex. 2, 5, 9.c.). Applicant received no formal training on what was required of her in her now senior security position (Tr. 127.), although apparently the government customer assessed her as qualified for the position. Applicant was confident in her ability to perform the duties of CPSO with the single exception of the information technology area ("I knew the NISPOM backwards and forwards . . . I was a great security officer"). (Tr. 129-30.) Work continued on multiple programs in the area and on the same information technology system as Applicant assumed all co-users had agreed. Around August 8, 2003, Applicant was promoted to a security manager position. She had security responsibilities for approximately 20 separate SAPs in the area (Tr. 114.), including SAP X which had by then more than 200 cleared personnel and seven full-time subcontractors involved and 13 separate areas to maintain. Security manager A retained control over staffing issues. (Ex. 2, Tr. 92-93.) There were only three ISSM's cleared for all the SAPs at the facility. (Ex. G.) While Applicant was a TS control officer and CPSO for SAP X, security issues surfaced involving SAP X, as follows.

Document Accountability Issues

When Applicant took over as CPSO for SAP X in May 2002, a significant amount of SAP X material was within the control of a special security officer with cognizance over SCI (hereafter the CSSO).[2] Previous security staff had treated all the material as SCI that required no accountability, when in fact there was special access required (SAR) material mixed in which required accountability.[3] (Ex. 2.) Applicant wanted all SAP X material within her area of cognizance. The CSSO resisted, but in late 2002, a decision was made to relocate all SAP X material from the vault to the SAP X area. Most of the material was eventually moved from the vault to the SAP X area in the spring of 2003. Due to closed storage space constraints within SAP X approved areas, some oversized material remained in the vault. The material included very large reel-to-reel tapes that were marked TS/SAR. (Tr. 107.) Neither Applicant nor security manager A brought those materials now in the SAP X area under accountability. Safes brought to the SAP X area "sat stagnant for many months" because of work demands, staffing issues, and the lack of any requests for the material. (Ex. 9.c.)

---

[2]SAP X involved collateral, SAP/SAR, and SCI information. Applicant testified that she was placed in charge of the SAP/SAR material in 2004. (Tr. 105.)

[3]Applicant explained that there was a misinterpretation within the SCI facility that TS/SCI did not need accountability, but that under the National Industrial Security Program Operating Manual (NISPOM) overprint, accountability of TS is required. (Tr. 90.) *See* NISPOM ¶ 5-201.a, which mandates TS control officials to maintain accountability records for TS information and to conduct an inventory annually.

In the spring of 2004, Applicant and a security associate began looking at the material moved from the CSSO's office. Problems with document control involving materials removed from the vault led Applicant to inform the cognizant MSAPSO in late April 2004 that a significant volume of accountable TS classified material pertaining to SAP X had not yet been brought into accountability.[4] (Ex. 2, Tr. 90.) The company was given a deadline of 30 days, which was later extended, to bring the material into accountability. A mass inventory was conducted in June 2004. Since Applicant was not fully cleared to the level of all the materials in the vault (Tr. 109.), the CSSO for the SCIF performed the inventory. (Ex. 10.c.) In late July 2004, Applicant notified the MSAPSO that her office had established a new accountability system, and that all documents and media had been brought into accountability as required.[5] Applicant also indicated that the company had educated all employees regarding the handling, storage, and accountability requirements for TS material. (Ex. 9.c.). Some classified, special access required reel-to-reel tapes were cut up and placed in bags that were left on a cart in the vault because the shredder broke before they could be destroyed. (Tr. 108.) According to Applicant, she kept SAP X's program security officer apprised of matters within her cognizance. (Tr. 109.)

Following a government security review (reinspection) in late January 2005, a 100% inventory was conducted of all items logged into accountability. Two items (a floppy diskette and a Zip disk) labeled TS could not be located. After an internal investigation, both media were found to be classified secret/NOFORN, and incorrectly entered into TS accountability. (Ex. 9.c)

In mid-January 2005, Applicant was replaced as CPSO for SAP X due to issues involving a LAN in her office, *infra*. On January 27, 2005, the CSSO for the SCIF at the company reported to the new CPSO for SAP X that there was classified material pertaining to SAP X in his vault. Because SAP X TS material had been outside of accountability between 2002 and 2004, an internal inquiry was conducted by company security to determine the facts surrounding what appeared to be inadequate accountability of TS material. (Ex. 9.c, 10.c.) The SAP materials in the vault included 8 millimeter tapes, reel-to-reel tapes, floppy disks, and other media and documents, which ranged in classification from Secret/SAR to TS/SAR/SI. The investigator determined there was SAP X material in the vault that should have been brought into accountability at the time of the mass inventory completed in 2004. Some of the items found had document control numbers from the previous accountability system used in the SCIF.

---

[4]Applicant indicated that she and a security associate discovered in the spring of 2004 that the document control numbers were inconsistent on SAP X material that had been brought from the CSSO's area. Due to computer issues, they were not able to confirm whether documents had been placed in accountability. In the administrative inquiry, the investigator reported that security manager A and Applicant admitted being aware of the existence of "hundreds of pieces" of accountable material outside of accountability. Applicant testified it was "thousands of pieces" of classified material. (Ex. 9.c.) Because of the volume, she asked for an extension of 180 days, but was given only 30. (Tr. 106-07.)

[5]Applicant indicated that most of the actual logging of the material was accomplished by security associates in her office. During the investigation, she provided a statement indicating that when the task was accomplished, she set a letter to the government indicating all classified material had been logged. (Ex. 9.c.)

One item found had been erroneously listed in accountability as having been destroyed, although there was no corresponding certificate of destruction for the material. SAP X's government program security officer and the MSAPSO with local oversight were notified of the unapproved storage in early February 2005, and the materials were secured. Applicant was among five employees identified as having had cognizance of the SAP X material and having failed to follow administrative procedures. In reporting the incident to the MSAPSO on March 2, 2005, the company indicated that those involved would receive a verbal warning concerning the improper storage and counseled about the responsibility to report security violations within their cognizance to the appropriate persons within the company and the government. (Ex. 10.c.)

LAN Issues

In early May 2003, an information system security manager (ISSM)[6] was hired for SAP X. His chain of command was within information technology security, and Applicant had no supervisory authority over him. (Tr. 101) The security network within Applicant's office was operating on old equipment and on an accreditation from May 2000 for joint usage. Around May 23, 2003, two branches of the U.S. military with special access programs in Applicant's office (customers #1 and #2) executed a co-utilization agreement giving customer #2 cognizant authority over the security space. The newly hired ISSM was told by his manager in information technology security that the co-utilization agreement covered AIS. (Ex. 5.)

Around August 2003, Applicant had arranged for SAP X (customer #3) to buy a new computer system (PC and server) for her office to support the program. The ISSM for SAP X submitted a plan to the cognizant MSAPSO for an AIS upgrade with a new operating system and hardware. The plan referenced the May 2003 co-utilization agreement, and specified that only customer #2's SAPs would be on the network. Work involving other services would be performed on stand-alone, dedicated systems. Based on his conversations with Applicant, the ISSM understood that there was very little activity involving other branches of the U.S. military. In October 2003, the MSAPSO approved the plan dedicating the network to customer #2's programs only. On the implementation of the new LAN in early March 2004, the data from the old network was placed on the new server without clearly identifying the programs or security levels of the information on the LAN. (Ex. 5.) Applicant was a user of the LAN in her security cognizance but she did not have administrative rights to the LAN. (Tr. 95.)

In the summer of 2004, the MSAPSO notified the ISSM that the co-utilization agreement for the new LAN did not cover AIS issues. Applicant again told the ISSM that

[6]In his memorandum of January 17, 2005, the information systems employee indicated he was hired as the information system security officer (ISSO). He was referred to as the ISSM (information system security manager) in the records documenting the investigation. He was a certified information systems security professional (CISSP), and Applicant was not. Applicant testified that she had been told by security manager A to stay out of computer security issues. (Tr. 115-18.)

the network contained no program technical information from other services.[7] Around August 23, 2004, the government program manager for SAP X[8] gave the ISSM special approval authority to include new nodes on the network, although the program manager retained overall authority for accrediting the network. (Ex. A.) In early October 2004, a new co-utilization agreement was effective with the final signature by four SAP customers,[9] stating that all data other than customer #2 data would be maintained on dedicated systems. During a companywide special access facility inspection by MSAPSO in October 2004, the facility was given a marginal rating. The information technology program was rated as unsatisfactory. (Ex. 2, Tr. 92.) Applicant testified that her program, SAP X, had only minor deficiencies which involved physical security issues (Tr. 92.). Evidence shows the co-utilization agreement on the LAN had to be revised to include a fifth customer (signatory). (Ex. 9.c.)

In November 2004, Applicant's employer submitted a request to the MSAPSO to modify the co-utilization agreement on the LAN in her area to allow the use of AIS to support all signatories. Applicant expressed concerns in December 2004 about the ISSM's time being spent on programs other than SAP X when SAP X had "major issues" that needed to be addressed before a government re-inspection.[10] (Ex. F.) The ISSM had been selected to head the re-inspection team for information security for all of the programs within MSAPSO's cognizance at the facility. (Tr. 97.) One of the LANs was running at the TS/SAR level to seven subcontractors and Applicant needed the ISSM to maintain the LAN. Applicant complained to information technology management, including the team leader in charge of the corrective action plan, that SAP X was not being adequately staffed. (Tr. 98)

On December 19, 2004, the team leader in charge of the corrective action plan expressed concerns to top security officials in the company about a security culture in the SAP/SAR security department that favored longtime employees over efforts to correct security issues. (Ex. G) In early January 2005, the ISSM notified the company of his intent to resign. (Tr. 100.) On January 12, 2005, the ISSM provided the MSAPSO

---

[7]During the investigation of the LAN problem in mid-January 2005, the ISSM indicated that Applicant told him that the old security network did not have any classified material on it. When the co-use problem was being addressed in the summer of 2004, he asked Applicant what information was on the LAN from other services and she indicated basic security administration information, receipt and dispatch records, and unclassified "HVSACO" information. In November 2004, he asked Applicant about the security level of material to be processed on the LAN, and she indicated unclassified HVSACO information to confidential/special access required. (Ex. 2.) Applicant testified discrepantly that when updated hardware was approved to the LAN in 2004, the ISSM labeled the LAN S/SAR because the system contained S/SAR information pertaining to SAP X. (Tr. 95.)

[8]The government program security officer for SAP X is distinct from the military special access program security office, which apparently had cognizance over SAP security issues involving its service's SAPs and not solely SAP X.

[9]The co-utilization agreement was apparently signed by two customers on September 23, 2004, by a third on September 27, 2004, and by the fourth on October 12, 2004. (Ex. 2)

[10]Applicant's testimony that her area had only two minor findings in the area of physical security is inconsistent with her demands for the ISSM's time because SAP X had some major issues.

with the configuration of the LAN that was approved to support only customer #2. The next day, the MSAPSO conducted a site visit and determined that the LAN was operating in violation of its protection level I accreditation and in violation of the co-utilization agreement for the facility. The LAN was suspended from operations and all user accounts but the ISSM's account[11] were locked based on suspicions of multiple SAP cognizant security agency data being commingled on the AIS. Applicant's special access was suspended by her employer (Ex. 5, 9.a, 9.c.) and by the MSAPSO as to the SAPs under its security cognizance pending an investigation. (Ex. 3, 4, 6.) Applicant was also formally suspended from her duties as CPSO for SAP X. (Ex. 10.c.)

An internal investigation was conducted over the next few days by Applicant's employer during which it was determined that the ISSM, Applicant, and three other security associates in the office had established accounts on the LAN and had confirmed access to data files on the system. Applicant expressed her belief to the investigator that data maintained on the server was not technical in nature, but included sterile addresses, receipt and dispatch records, TS accountability registries, access lists, forms, correspondence, and other unclassified security-related documents. She told the investigator that she assumed that the LAN was approved to the S/SAR level, and she received assurances from the ISSM when the new server was added that all had been approved. In her mind, the ISSM was responsible for the LAN. Security manager A did not have an account on the LAN, and she believed the ISSM and Applicant shared security responsibility for the system, although there was a general opinion in the SAPSO that security manager A did not provide adequate direction or oversight of the security office. Due to inadequate documentation, the investigator could not fully establish a trail showing approval of the AIS LAN and the co-utilization agreement. (Ex. 5, 9.c.)

On January 18, 2005, the MSAPSO reviewed the data, both shared and local, on the LAN server and local client hard drives. In addition to unclassified information pertaining to several of its contracts, to old or unrecognized SAP contracts pertaining to activity outside the current co-utilization agreement, and database files that supported current and past SAP customers, the MSAPSO found classified information up to the TS/SAR level, and classified associations in receipt and dispatch databases, which was outside the approved accreditation (protection level 1) for the LAN and in violation of the existing co-utilization agreement for the facility. The MSAPSO could not rule out the possibility of compromise of classified data since all users had not been approved for access to the data on the system. The security LAN would have to be formally dis-accredited and any affected media destructed. (Ex. 6, 9.c.)

[11]Applicant maintains that the ISSM was responsible for the LAN found to be in violation. Yet, his access was not suspended. (Tr. 100-01.) She assumes that the ISSM knew the LAN was not going to pass on the reinspection, and that he called in the MSAPSO investigator to divert the attention from him to her. (Tr. 102.) No disciplinary action was taken against the ISSM.

Laptop Issue

Sometime during the latter half of 2004, the ISSM found seven laptops in SAP X's area. The laptops were not marked on the outside, and hard drives were not marked on those computers that had hard drives. He secured the laptops and notified the government and Applicant about the laptops. Applicant knew that the previous ISSO had two laptops that were unclassified and used for travel. She assumed there was a policy in place for the laptops to be held in the SAR area. After she was told about the other laptops in 2004, she assumed they came from an unclassified area and relied on the ISSM to obtain procedures for the use of the laptops in the SAR area. (Ex. 9.c.) After an eighth laptop was found during the government's re-inspection in January 2005, the company conducted an internal investigation into the laptops. In a document dated May 2001, the cognizant security office had provided one-time-use approval on a case-by-case basis, but the approval did not specify a laptop by serial number or include the appropriate form. Two hard drives containing classified material were of the correct model for the laptops, but it could not be validated whether those hard drives were from the laptops approved for one-time use. Of the two laptops that had internal hard drives, only one could be accessed and a basic search returned no results that would indicate classified material was on the laptop. Because of turnover in the SAP security department and poor record keeping, individual responsibility could not be determined. (Ex. 10.a.)

Administrative Inquiry

Following its review of the incident involving the LAN, the MSAPSO issued a memorandum on April 4, 2005, notifying Applicant's employer that her SAP accesses remained suspended pending a final adjudication of her clearance eligibility. The MSAPSO determined that as TS control officer, Applicant was directly involved in the mishandling of TS/SAP materials, that her actions contributed to the unauthorized exposure of classified SAP material to non-accessed individuals, that she knowingly violated established co-utilization agreements between DoD services through the use of an unauthorized LAN, and that she willfully withheld classified materials from CSA inspection and/or oversight. (Ex. 7.)

Over the March to June 2005 time frame, the company conducted its inquiry into the security issues involving SAP X at the facility. Applicant was interviewed over the March 16 to 18, 2005 time frame about the unaccountable documents. Applicant averred that she had told security manager A and the CSSO when she took over security responsibilities for SAP X in 2002 that all SAP X material had to be brought under her cognizance, but the CSSO wanted to retain the TS material. Applicant admitted that after management decided to relocate the material from the vault to her program area, SAP material resided in the program area outside of accountability until she notified the government. Applicant explained that the delay in obtaining the program material and bringing it into accountability was due to lack of management oversight and support, including from security manager A, and a lack of trained personnel to conduct daily operations. She indicated that an effort was made to identify material for destruction back in 2003, but that "with the multitude of issues going on at the time,

understaffing, and having no destruction facility," items sat waiting for destruction. (Ex. 9.c.)

On March 21, 2005, Applicant was interviewed about the laptops. She expressed no knowledge of unclassified laptops being used or stored in SAR areas. She provided a written statement the following day in which she explained that she learned about the laptops when she came onto the program, and she assumed that there was a program in place for the laptops to be held in the SAR area. Due to other demands on her time involving SAP X, she relied on the ISSM to deal with the issue. Applicant highlighted another risk to her program inasmuch as company employees not briefed to SAP X were used to courier program material and to retrieve mail from the SAP X sterile post office box. As of July 2005, the company was conducting an internal inquiry into that issue and relocating the post office box to prevent the possibility of future compromise. The available records contain no indication as to who directed personnel, who had not been briefed, to courier or retrieve SAP material. (Ex. 9.c.)

On March 28, 2005, the CSSO indicated that shortly after he was hired in October 2004, he focused on identifying, compiling, and organizing the records for the SCIF, and that in November 2005, he had requested Applicant's assistance in identifying SAP X materials in the vault for destruction. Applicant responded that she was working on an inspection corrective action plan for her area following the marginal facility rating in October 2004, and would defer the issue to security manager A. As reflected in an email response of November 12, 2004, Applicant informed the CSSO that it would be okay to move the material around in the vault and she proposed a date of February 1, 2005, after the re-inspection, to start destruction. The CSSO responded that he could work with that timetable, but untimely destruction was a security problem that he planned to address as part of his area's overall self-inspection. The SAP X material remained in the vault until after the January 2005 re-inspection, when Applicant was replaced as CPSO for SAP X. The CSSO raised the issue with the new CPSO, and the material pending destruction was removed. (Ex. 9.c.)

During the company's inquiry, a security associate in the SAPSO expressed concerns about minimal security training. Although she characterized Applicant as "very knowledgeable" about security issues, she corroborated Applicant's assessment that security was forced to do more with less, even to bend the rules to ensure that program demands were met with the limited resources available. The security associate admitted that she and Applicant were aware that TS materials had not been brought into accountability in a timely manner due to personnel shortages. This security associate recalled all materials were brought into accountability and destroyed as necessary. However, when presented with some destruction documents from the 2004 time frame, the employee could not identify those documents in the accountability system's records, which led the investigators to believe that TS material had been destroyed without first being brought into accountability. Another employee, who had provided administrative support for the SAP X from October 2003 to August 2004, recalled that a significant amount of TS material was destroyed during an atmosphere that she described as chaotic. (Ex. 9.c.)

No information was obtained during the investigation that would suggest SAP X information was released outside approved program areas of the CSSO's vault. However, the area staff could have been inadvertently exposed to SAP X information, so they executed inadvertent disclosure statements. The company reinforced the requirement to timely report suspected deficiencies to proper government cognizant authority. The investigator concluded that security manager A and Applicant were negligent in that they were aware of, but failed to report, the existence of "hundreds of pieces" of accountable material to the government and bring it into full accountability. The investigator also concluded that both security manager A and Applicant "purposefully" hid SAP X material pending destruction in the CSSO's vault during the January 2005 timeframe to avoid detection by the government security review team, and that both Applicant and security manager A admitted to it. Furthermore, Applicant and a security associate made incorrect statements about materials being brought into full accountability before destruction. Applicant, security manager A, and the security associate who dealt with the destruction were felt to have been deceptive during the inquiry to protect their jobs. (Ex. 9.c.)

On June 2, 2005, the MSAPSO recommended to military adjudication personnel that Applicant's and security manager A's access to SAP be revoked for negligence in their handling and lack of control over SAP material, for knowingly putting material at risk of compromise by placing SAP material in an area where non-accessed employees had control of the items, for attempting to hide unaccounted items from a MSAPSO security review team, and for failing to exercise appropriate management oversight over day-to-day security processes at the company. (Ex. 8.) Applicant, who had continued to work for the company in security in an unclassified area following the suspension of her special access, started working as a configuration management specialist at a different facility within the company in June 2005. (Ex. 2, Tr. 149-50.)

Even after her SAP access had been suspended, Applicant still had the support of a security manager, and of managers of other government programs for whom Applicant had provided special security needs. She was knowledgeable about security issues and honest with them in her intent and actions. A program manager for a national intelligence mission found her to be "dependable, reliable, hard-working and conscientious." In his opinion, Applicant acted consistent with the sensitive nature of the program and recognized the need for "perfect OPSEC practices." In June 2005, another program manager, who had a close working relationship, described Applicant as "an outstanding manager, with superior knowledge of special security." Yet another program manager at the company considered her removal from her security duties to be a loss for himself and other government contract programs at the company. (Ex. 2.)

Applicant's employer notified the Defense Security Service of the results of its administrative inquiry on July 7, 2005. (Ex. 9.c.) On March 9, 2006, Applicant was interviewed by a government investigator about the security problems when she was CPSO. Applicant maintained that she was issued only two minor violations in the October 2004 inspection, but the information technology at the facility was rated as unsatisfactory. Applicant had complained to the special security officer that she had only two employees with whom to run 20 programs and was unable to keep up with

regulations because she was understaffed. After she found a pile of unlabeled disks in her area, she notified the MSAPSO of her complaints. As for SAP X material being in the vault in January 2005, Applicant responded that the material should not have been there. She opined that the ISSM had disclosed the company's security problems to his neighbor, who had been involved in the MSAPSO inspections, to get back at the company that had denied him a promotion and to shift the blame from himself to her.[12] Applicant expressed her belief that the military acted to protect itself because of its own lack of cognizance. She asserted she was made a "scape goat" for the mistakes of others, and denied any responsibility for the security violations.

In a January 12, 2008 statement to DOHA, Applicant indicated that the ISSM, not she, had administrative rights to the LAN. Personnel were given accounts on the LAN that should not have had the access, but were "strong armed" by her former supervisor, security manager A. She reminded DOHA that she had notified the cognizant MSAPSO that the company was not complying with the requirements to control and store information classified TS/SCI/SAR. Applicant indicated that supervisors were put in the compromising position of having to clean up programs that she had not been cleared on. (Ex. 2.)

Applicant has been dependable in meeting deadlines and in adhering to company procedures in her current position. (Ex. 2.) In her performance review following her first full year in configuration management, Applicant was assessed as having achieved all her job objectives, with her only weakness being a lack of experience in the field. (Ex. C.) In 2007, she exceeded job expectations in several areas (implementing programs, process, meeting utilization targets). She brought order to a dysfunctional program and did an excellent job ensuring timely release of hardware and software documentation and internal data. (Ex. D.) Again, in 2008, she exceeded some objectives, with significant cost savings to a program. (Ex. E.) A coworker familiar with her performance as a security manager and in her present position in configuration/data management considers her to be dedicated and professional in carrying out her duties. (Ex. 2.)

Applicant's TS security clearance has been suspended because of the security violations in 2004/05. She requires a secret-level security clearance for her present duties. (Tr. 165-67.) Applicant denies that she deliberately hid SAP X material in the vault. The vault was on the inspection list for reinspection and it had been cleared to store SAP X material. (Tr. 104) She also cannot understand why the ISSM was not disciplined because of the unauthorized use of the LAN. (Tr. 101-02)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security,

[12]Applicant indicated in January 2008 that she had speculated as to the motives of the former ISSM. (Ex. 2.) She testified at her October 2009 hearing that the ISSM and the MSAPSO investigator had worked together in the past at the local military base and were "very close friends." (Tr. 93-94)

emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are required to be considered in evaluating an applicant's eligibility for access to classified information. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture. Under Directive ¶ E3.1.14, the government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion as to obtaining a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information. Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Handling Protected Information

The security concern for handling protected information is set out in Guideline K, AG ¶ 33:

> Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

The Government alleged in SOR 1.a that Applicant was found responsible for two security violations as a result of an inspection conducted of a SCIF at her place of employment. Applicant denies being cited for any security violations as a result of that inspection. To the contrary, she contends that SAPs under her security cognizance had only two minor findings that had to be corrected before the re-inspection. The inspection report was not made available for review, and the nature of the alleged security violations is unclear. The Government submitted in closing argument that the violations concerned the LAN and the vault. But the evidence shows that the only issue known about the LAN at that time was that the co-utilization agreement finalized in October 2004 had to be revised to include a fifth signatory. The ISSM was working with the MSAPSO to correct the issue. As for the vault, problems with accountability known to the MSAPSO had been addressed during the summer of 2004. The issue with SAP X TS/SAR reel-to-reel tapes and other SAP X material remaining in the SCIF did not surface until late January 2005. The evidence instead shows that the laptops were found in SAP X's area during the government inspection in October 2004. But Applicant denies previous knowledge of classified laptops in her area, and they remained secured pending the ISSM acting on her direction to obtain approvals. There is no evidence that she was personally cited for a security violation relating to the laptop issue. To the contrary, individual responsibility could not be determined following her employer's investigation. In short, the evidence fails to establish SOR 1.a.

As for the security issues involving the vault and LAN, which are covered in SOR 1.d, the evidence establishes that while Applicant was the CPSO for SAP X and TS control officer, she mishandled classified SAP material in failing to ensure that TS/SAR material was brought into proper accountability before the summer of 2004. While Applicant is credited with pushing for the removal of SAP X classified material from the SCIF into the SAP X area by spring of 2003, and for informing the MSAPSO in April 2004 that a large volume of classified material remained outside of accountability, she and security manager A were culpable for violating security regulations in that they knowingly permitted hundreds, if not thousands, of classified items to remain outside of accountability until the summer of 2004. Under ¶ 5-201 of the NISPOM, the TS control officer is required to maintain accountability records for TS information. AG ¶ 34(g), "any failure to comply with rules for the protection of classified or other sensitive information," clearly applies.

Also, Applicant was asked by the CSSO in November 2004 to remove classified material pertaining to SAP X from the SCIF. Because she was focused on the upcoming government reinspection, she told the CSSO that she would defer the matter to security manager A since the inspection corrective action plan took priority. In response to his request for a timetable, Applicant suggested February 1, 2005, after the reinspection, and the CSSO did not object. As a result, material remained in the vault until after she was replaced as CPSO. Applicant's employer concluded after its investigation (and the

MSAPSO concurred) that Applicant had willfully withheld classified materials from CSA inspection and/or oversight:

> Further, information was obtained during this investigation indicates some [SAP X] material pending destruction was purposefully hidden within the CSSO's vault during the January 2005 timeframe to avoid being detected by the USG Security Review Team. Both [security manager A] and [Applicant] admitted to this, thus exposing non-program-briefed individuals to [SAP X] information. (Ex. 9.c.)

The records available for review show that Applicant knew that SAP X material, which was classified up to TS/SAR, was kept in the CSSO's vault pending destruction as of January 2005.[13] But she denies willful concealment from the CSA. Applicant's uncorroborated testimony is that the vault was included on the inspection list. (Tr. 152-54.) The fact that the CSSO brought the unapproved storage to the attention of the new CPSO for SAP X would indicate that the classified material was not discovered during the reinspection. It is possible that the material could have gone undetected. It would not appear that material was moved into the vault solely to conceal it from the upcoming inspection. Materials were apparently in the SCIF because of their size or lack of space to accommodate all items for destruction. That having been said, Applicant knew about the upcoming reinspection, and that persons with access to the CSSO's SCIF had not been briefed to SAP X. By leaving the SAP X material classified up to the level of TS/SAR in the vault, including in green bags on a cart, she risked being found in violation of accountability and destruction requirements in the upcoming inspection, presuming the inspectors had access to the vault. More important, she knew or should have known that she placed SAP X classified material at risk of compromise by non-accessed employees while it was in the vault. Not all persons with access to the vault

---

[13]Applicant testified about the materials found in the vault in the fall of 2004, as follows:

> I was given 30 days to bring thousands of pieces of classified into accountability. The problem with a lot of this was we didn't have containers to put it in, it was thrown in the vault. When I say things were thrown in the vault, they were thrown in the vault. They were not in containers. I don't know if you are familiar with Ampex tapes. Ampex tapes are reel to reel test tapes. They are about that big, they have a small reel in the middle and the rest is all tape, it's huge. It's tapes that you would take out in the field during testing. There are hundreds of these. These do not fit in containers. They were TS/SAR/SI, that was the stamp on them. What we did was we had an approved shredder in the back, we had a very cognizant [SAP X] engineer come down and say you can keep that, you've got to get rid of this, you can keep that, you know, things we needed to keep for historical data. We destroyed multiple of these tapes. They are all on certificates of destruction with two people signing off on the tape. During that time, the shredder broke. We advised the government that the shredder had broke [sic] and we couldn't get, there was no other way to destroy this material. The way you destroy it is you actually take a ceiling like this and you pull the tape and you end up with a pile of tape. You usually have to cut it to fit it into garbage bags, so it would fit into garbage bags. This is the material that they have that I didn't show to the United States government because we had two garbage bags full of shredded Ampex tapes that we couldn't shred because the shredder wasn't working at the time. This was what was found in the vault, to my knowledge . . . ." (Tr. 107-08.)

had been briefed on SAP X. While the CSSO had primary responsibility to ensure that the material was properly protected once he found it in the vault in the fall of 2004, Applicant violated her obligation to protect classified material within her security cognizance. *See* NISPOM ¶ 1-200 (stating, "contractors shall protect all classified information to which they have access or custody"). AG ¶ 34(a), "deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences," applies to the extent that disclosure because of Applicant's negligence cannot be ruled out. There is no evidence proving access, deliberate or inadvertent, by an individual non-accessed to SAP X. AG ¶ 34(b), "collecting or storing classified or other protected information at home or in any other unauthorized location," and AG ¶ 34(g) clearly apply.

The company's investigator found Applicant deceptive in that she had assured the MSAPSO in the summer of 2004 that all materials had been brought into full accountability, when "new program material" ranging in classification from unclassified to TS had been found within the CSSO's vault in January 2005. An employee who provided administrative support to the SAPSO from October 2003 to August 2004 expressed her belief that the destruction was only 1/3 complete when she left the office. It is unclear whether the "new" information is from this time frame. During the inquiry, it was discovered that several pieces of accountable material had been destroyed without first being brought into accountability, but the information does not show that Applicant knew that her security associates had failed to log those particular items. As a result of the company's investigation over the March to June 2005 time frame, two items were placed into TS accountability; the rest were determined to be non-accountable. Given that hundreds or even thousands of documents had to be logged into accountability during the summer of 2004, I cannot conclude based on the evidence that Applicant lied when she told the MSAPSO that all items had been brought into accountability.

Concerning the LAN within the SAP X area, the co-utilization agreement in place as of October 2004 specified that only customer #2 data would be maintained on the LAN dedicated systems. During an effort by the ISSM to get the LAN approved for security administrative functions to support multiple SAPs, the LAN was discovered to be operating in violation of its protection level 1 accreditation and the established co-utilization agreement. Multiple SAP CSA data was commingled on the AIS. No SAP technical data associated with any of the company's customers was identified on the LAN, but the LAN data included classified combinations up to the TS/SAR level and classified associations in receipt and dispatch data bases. Applicant had told the ISSM that the system contained only unclassified security administrative data. Whether or not she knew that classified data was on the system, she was negligent in failing to ensure that the LAN was in compliance with its existing protection level and co-utilization agreement. Deficiency in her AIS knowledge in comparison to the ISSM, and the fact that she did not have administrative rights to the LAN, do not excuse her failure to comply with her oversight responsibilities in all areas of security under her cognizance. AG ¶ 34(c), "loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware,

software, drive, system, game board, handheld, 'palm' or pocket device or other adjunct equipment," applies in that her negligence led to material up to TS/SAR being loaded onto the office LAN, in violation of the protection level for the system. Furthermore, her failure to exercise her security responsibilities over the LAN and its contents falls within AG ¶ 34(g).

Concerning the potentially mitigating conditions, five years have passed since Applicant's violations of security procedures. While she satisfies the first component of AG ¶ 35(a), "so much time has elapsed since the behavior," it is difficult to mitigate the Guideline K concerns solely on the basis of the passage of time. She has handled information in her new position in data/configuration management appropriately, but with her TS clearance suspended, there is no track record of subsequent compliance with the rules and regulations concerning classified information that would lead one to conclude that the violations are not likely to recur. AG ¶ 35(a), "so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment," does not adequately mitigate the serious security concerns.

AG ¶ 35(b), "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities," does not apply in the absence of any effort by Applicant to obtain security training or to accept responsibility for her own lack of security oversight. Whether or not the ISSM should have been disciplined or held partially responsible for the LAN violation, Applicant would have gone a long way toward showing reform had she at a minimum acknowledged the role she played in the LAN violation. She provided inaccurate and conflicting information to the ISSM about the level of classified information on the LAN. Furthermore, she disputes that she knowingly put material at risk of compromise by placing SAP material in an area controlled by non-accessed employees. (Tr. 151) Given she did not have access to the vault, she likely did not put the classified SAP material in the vault herself. But certainly by the fall of 2004, if not before, she knew it was there. She testified that she had documentation from probably the early 1990s indicating that the vault was approved for the storage of SAP X SAR material. (Tr. 104) Assuming the authorization was still valid, the method in which the TS/SAR tapes were stored (garbage bags) left the material vulnerable to unauthorized access. Moreover, there is no evidence that she brought the storage problems to the attention of the MSAPSO in the fall of 2004.

Applicant's argument for mitigation under AG ¶ 35(c), "the security violations were due to improper or inadequate training," is not particularly persuasive. While she did not have had any formal training when she was started in the SAPSO at the company, she had enough on-the-job training by 2002 for the government to approve her as CPSO for SAP X. Her lack of expertise in the AIS explains to some extent her reliance on the ISSM in seeking the necessary approvals for the LAN upgrade, but it does not justify her failure to provide accurate information to the ISSM about the level of classification on the LAN and whether it included program data from multiple customers. Applicant testified at her hearing that she knew the NISPOM "backwards and forwards."

Several program managers, for whom Applicant provided security before her access was suspended in January 2005, found her to be very knowledgeable in special security matters.

Applicant's violations are extenuated in part. Applicant had security responsibilities for about 20 SAPs when the workload on SAP X was increasing. Her requests for adequate staffing were only minimally supported. The ISSM was hired for SAP X in May 2003, but he had duties during the fall of 2004 that took him away from maintaining the LANs in Applicant's area. During the summer of 2004, there were only a few security associates in the office to bring hundreds if not thousands of documents into accountability. There were systemic problems in security within the facility at the time, as evidenced by its apparent marginal inspection rating in October 2004. But however difficult the working environment, Applicant had an obligation to her government customer to protect the sensitive information within her security cognizance. Her burden of reform is not fully met where she accepts little responsibility for her own violations. Work demands do not justify the delay in reviewing the contents of SAP X material removed from the vault, or the improper storage of TS/SAR materials in a SCIF where persons not briefed on the program could gain unauthorized access.

Personal Conduct

The security concern for personal conduct is set out in Guideline E, AG ¶ 15:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

Based on their respective security inquiries into the security violations that led to the suspension of Applicant's access to SAP, the MSAPSO and Applicant's employer concluded that Applicant willfully withheld classified materials from CSA inspection or oversight or both. (Ex. 7, 8, 9.c.) Presumably, both are referring to the knowing storage of the TS/SAR material in the vault over the fall of 2004 until after the reinspection. Such untrustworthy or unreliable behavior would raise serious personal conduct concerns under AG ¶ 16(d):

> Credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of: (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sens

Applicant has consistently denied any intent to hide the SAP X classified material in the vault. As discussed *supra*, Applicant did not remove the material from the vault over the fall of 2004. While the company investigator indicated that both security manager A and Applicant admitted that SAP X material pending destruction was hidden in the CSSO vault to avoid detection, the investigator's summaries of the respective interviews did not contain the alleged admissions. Written statements were provided by both security manager A and Applicant, which were attached to the investigator's report. Neither statement contains an admission of knowing concealment of material from inspectors. Applicant has not denied that some material remained in the vault. The evidence before me for review falls short of proving wilful concealment. AG ¶ 17(f), "the information was unsubstantiated or from a source of questionable reliability," applies as to SOR 2.a.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of his conduct and all relevant circumstances in light of the nine adjudicative process factors listed at AG ¶ 2(a):

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept.

Applicant's TS clearance and her access to SAPs were suspended because of her involvement in the mishandling of classified TS/SAP materials while TS control officer and CPSO for SAP X. She placed TS/SAR material at risk by leaving it in a vault accessed by individuals who had not been briefed on the program(s). She neglected her responsibilities to timely place into accountability and destroy where appropriate sensitive information involving SAP X that had been brought out of the SCIF into her area. As for the LAN, she told a government investigator that she assumed the LAN was approved to the S/SAR level, and she relied on the ISSM to obtain the approvals for the new hardware. While there was old information on the LAN, database files were identified that supported current customers beyond customer #2, including receipt and dispatch records and SAP door and container combinations. TS accountability records were on the system pertaining to customer #2. She has not fully addressed the discrepancy between her reported understanding of what was on the system and what was found. The overall security posture at the facility was a contributing factor in that

security took a backseat to other program demands, and Applicant had a demanding, if not overwhelming, workload. But Applicant had enough experience in security to understand that she should not bend the rules by storing classified material in an unapproved location and risk compromise. Despite the passage of time since the violations, and some very favorable references, I am unable to conclude based on the record before me that it is clearly consistent with the national interest to grant or restore access to classified information for Applicant.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	For Applicant[14]
Subparagraph 1.c:	Against Applicant
Subparagraph 1.d:	Against Applicant
Subparagraph 1.e:	For Applicant[15]
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

Elizabeth M. Matchinski
Administrative Judge

[14]SOR 1.b is found for Applicant in that it references solely an administrative action taken by her employer and does not allege any specific violation.

[15]There is no evidence of a final decision on her special programs access. Furthermore, SOR 1.e does not allege any violation committed by Applicant.