DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 09-00905
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Alison O'Connell, Esquire, Department Counsel

For Applicant: Sheldon I. Cohen, Esquire

September 20, 2010

Decision

O'BRIEN, Rita C., Administrative Judge*:*

Based on a review of the case file, pleadings, and exhibits, I conclude that Applicant has not mitigated the security concerns raised under the guidelines for handling protected information, personal conduct, and use of information technology systems. Accordingly, his request for a security clearance is denied.

Applicant submitted an Electronic Questionnaire for Investigations Processing, which he signed on July 21, 2005. After reviewing the results of the ensuing background investigation, adjudicators for the Defense Office of Hearings and Appeals (DOHA) were unable to make a preliminary affirmative finding[1] that it is clearly consistent with the national interest to grant Applicant's request for a security clearance.

[1] Required by Executive Order 10865, as amended, and by DoD Directive 5220.6 (Directive), as amended.

On January 14, 2010, DOHA issued to Applicant a Statement of Reasons (SOR) that specified the basis for its finding: security concerns addressed in the Directive under Guideline K (Handling Protected Information), Guideline M (Use of Information Technology Systems), and Guideline E (Personal Conduct) of the Adjudicative Guidelines (AG).[2] Applicant signed his notarized Answer on February 4, 2010. He denied all allegations in the SOR. He also requested a hearing before an administrative judge. Department Counsel was prepared to proceed on March 24, 2010, and the case was assigned to me on March 29, 2010. DOHA issued a Notice of Hearing on April 14, 2010, and I convened the hearing as scheduled on May 19, 2010.

During the hearing, the Government offered five exhibits, which were admitted as Government Exhibits (GE) 1, 2, 4, and 5, without objection.[3] I admitted GE 3 over Applicant's objection to two pages. Applicant testified, presented the testimony of two witnesses, and offered 31 exhibits, admitted as Applicant's Exhibits (AE) A through EE. DOHA received the transcript (Tr.) on May 28, 2010.

Procedural Issues

On April 13, 2010, Applicant requested to have witnesses testify by telephone. Department Counsel did not object to the telephone testimony. I held a telephone conference call with both parties on April 14, 2010, and granted Applicant's request.[4]

Findings of Fact

After a thorough review of the pleadings, the testimony, and the record evidence, I make the following additional findings of fact.

Applicant is 27 years old, single, and has no children. He graduated from college *cum laude* with a bachelor's degree in economics and international affairs in 2005. Since 2005, when he began working for a defense contracting company, he has received training in Department of Defense functional areas and holds a certification in life-cycle logistics. He held an interim security clearance in 2005 while working for Company A, a defense contractor, but did not work with classified material in that position. In 2006, he accepted employment with another defense contractor, Company B, as a logistics analyst. He worked for Company B from 2006 to 2008. Since November 2008, he has worked for Company C, a defense contractor, where he holds the positions of senior logistics manager and assistant facility security officer (FSO). In

[2] Adjudication of this case is controlled by the Adjudicative Guidelines (AG), which apply to all adjudications or trustworthiness determinations in which an SOR was issued on or after September 1, 2006.

[3] Applicant objected to pages 110 and 111 of GE 3, the courier instructions, on the grounds that he had not seen them before he received them during discovery for this hearing. However, the record indicates that he received this information in either December 2007 or January 2008. (*See* footnote 11, *infra*)

[4] *See* Directive, Enclosure 3, §§ E3.1.9 and E3.1.10.

April 2010, he completed coursework for FSO certification and is qualified as an FSO. He currently holds a security clearance. (GE 1; AE K – Q, R - U; Tr. 64-80, 136, 140-141, 155)

According to Company B's FSO, Applicant "received necessary security training in October 2006" when he joined Company B. On October 16, 2006, Applicant read and signed four documents titled, "General Security Briefing,"[5] "Reporting of Adverse Information," "Counterintelligence Briefing," and "Foreign Travel Defensive Security Briefing." The General Security Briefing[6] ended with the following statement above the signature line: "By signing this form I acknowledge my security responsibilities as explained to me and agree to observe security rules and regulations involved." At the hearing, he testified that he did not receive a briefing about security, the National Industrial Security Program Operating Manual (NISPOM),[7] Company B's Standard Practices and Procedures (SPP) for security, or about the information in the documents he signed. He did not receive a copy of the documents. (GE 3; Tr. 82-83, 85-87, 230)

While employed by Company B, Applicant was transferred from his original job at Site C to Site A, where the testing and evaluation (T&E) of military equipment was conducted. He provided daily reports on the T&E, and acted as liaison to the project's program management office, which was located at Site C. His military supervisor for the T&E project was Major A, a Marine Corps officer, whose office was at Site C. Applicant provided daily reports to Major A about each day's testing. His reports were not classified; however, test results, images, and videos of the testing were classified. (Tr. 81, 89)

On August 8, 2007,[8] Major A told Applicant he wished to see several compact disks (CDs) showing testing of the equipment. He told Applicant to obtain these secret-

[5] The two-page General Security Briefing contained in GE 3 is partially illegible. Upon request for a more legible copy, Department Counsel provided to Applicant's counsel and to me her own transcribed account of the two pages. I have not used this account, as it was prepared by one of the parties. In referring to this document, I rely only on those sections that are legible, or that were read into the record and agreed to by Applicant during the hearing.

[6] The General Security Briefing contained the following relevant sections: Section 9, which prohibits reproduction of classified material without the prior consent of the FSO and without entering the reproduction into accountability records; Section 16, which prohibits holding classified materials overnight, without special provisions; and Section 19, which requires immediate reporting to Security of the following, *inter alia*, "Loss, compromise or suspected compromise of classified material by yourself or any other employee or subcontractor employee." (GE 3)

[7] *See* Department of Defense Manual 5220.22-M, *National Industrial Security Program Operating Manual* (*NISPOM*). (February 28, 2006)

[8] The record is contradictory as to when Applicant brought the CDs to Major A. Applicant testified that he provided the CDs to Major A in August 2007. However, emails among the involved civilians and military members indicate Applicant gave the classified CDs to Major A in June 2007. (AE G; Tr. 94)

level CDs from Mr. B, who was in charge of the ballistics program at Site A. Major A also told Applicant to put the CDs in the safe[9] in Applicant's office, and later, he would let Applicant know when he should take them to the Major's office. Mr. B told Applicant that he would not release the classified CDs until Applicant had a courier card authorizing him to transport them, and Applicant should contact his FSO about the courier card. Applicant's FSO informed him that he did not need a courier card to transport classified information from one cleared facility to another cleared facility.[10] However, she faxed a courier card to Applicant. Once Applicant had the courier card, Mr. B. had Applicant sign a form, which Applicant thinks was a release or receipt indicating that the material was being released to him. Mr. B. kept the form. He then handed Applicant a locked, zippered pouch that held a plastic container with approximately 20 CDs. The container was marked Secret, but Applicant does not remember if the individual CDs were marked. Each CD contained three videos and approximately 20 images. Each video began and ended with a Secret marking. Applicant returned to his office, placed the pouch in the safe, and called Major A to let him know he had the CDs. Major A then told Applicant to bring the CDs to the Major's home at Site B, instead of to his office. He also told Applicant not to tell anyone about bringing the CDs from Site A to Site B. Applicant drove to Major A's home with the CDs in the locked pouch. (GE 2**,** 3; AE H; Tr. 94-101; 163-166, 174, 260)

After receiving the pouch, Major A told Applicant that he needed the CDs in order to prepare a briefing about the equipment testing. In his statement to the NCIS investigator, Applicant stated, "[Major A] informed me he was burning copies of the CDs." Applicant said, "I remember [Major A] continually told me to keep quiet about the CDs and what we were doing was technically wrong." Applicant's understanding was that, "He [Major A] didn't want a lot of folks to know about it." He testified that the Major indicated it was bringing the CDs to his home that was "technically wrong." Applicant testified that he did not pursue this remark for several reasons: he never questioned the Major; the Major was an expert who had written the security classification guide for the program; Applicant respected and admired him; and he did not think Major A was doing anything wrong. Applicant did not report his own actions, the Major's actions, or Major A's comments to any authority. He testified, "I didn't understand what he meant and I didn't ask questions. I wasn't in the position to ask him what he meant. I did not have a relationship like that with him. It was – I was very intimidated by him as well. He was very powerful. He was very – you know, I just didn't really talk to him." As to why

[9] During his NCIS interview, Applicant described this safe as a "file cabinet." His signed statement says he told the investigator it was not a classified container. However, Applicant denies that he said that, and states that the investigator inserted that comment. Applicant testified that he signed it despite the inaccuracy because he was under a lot of stress and overlooked it. The container where Applicant stored the CDs is the only one in that office. On December 18, 2007, the Company B FSO verified that the cabinet in Applicant's office was "an approved GSA safe there physically in the office, with an X09 lock and that the level of that safe was SECRET." (GE 2; AE EE; Tr. 224-225)

[10] Applicant testified that he believes his FSO thought that he was bringing the CDs to Major A at his office in a cleared facility. At that point in time, Major A had not yet requested Applicant to bring them to his home.(Tr. 258-259)

he brought the classified CDs to the Major's house, he testified, "I was following orders." (GE 2; Tr. 102-105, 174, 176, 181-183, 205, 207-208, 234-235, 238)

Applicant saw Major A open the pouch, remove the CDs, put them into his computer, and start downloading the contents. Applicant did not see any markings on the computer indicating it was cleared for use with classified material. Before Applicant left, the Major said he would call him the next day to let him know when to pick up the CDs. Applicant did not receive a receipt for the CDs. Major A called Applicant the following afternoon, and Applicant drove back to the Major's house and retrieved the CDs. There is no evidence that Applicant obtained a receipt from Major A when he retrieved the CDs. Applicant told Major A that he planned to put the CDs in the safe in his office at Site A. He drove directly to his office after leaving Major A's home. (Tr. 102-105, 174, 181, 187)

When Applicant arrived at his office at Site A, he did not store the CDs in the safe immediately. He used his unclassified computer to view the videos and images on eight of the CDs, and he downloaded the data onto his work computer. He testified that he thought if the Major had put the data on his computer, then Applicant could do the same. He believed that since he held a security clearance, he was entitled to view them. He also testified that he thought he was allowed to place the secret data on his computer because it was password protected, and no one else had access to it. He wanted to have the testing images because he was too busy to be able to view the testing himself, and having the images would allow him to answer customer questions about the testing. In addition, one of his assignments was to train two Chief Warrant Officers (CWOs) about his job, and he thought it would be helpful if he had the data on his computer during the training. Applicant testified that he always brought his work computer home with him because he worked long hours, and he continued his email correspondence after work hours. Applicant returned the CDs to Mr. B two days later. Applicant testified that, before he couriered the secret CDs, he had never handled classified material or been informed about classified computers. (Tr. 105-110, 194, 197-204, 220)

In September 2007, Applicant was transferred to State A to train the CWO who would be taking over his job. Applicant was still reporting to Major A, and still preparing daily test reports. The company had no knowledge of these events, and in October, Applicant received laudatory emails from his company supervisor and a vice-president, congratulating Applicant because Major A was very satisfied with his performance. On November 29, 2007, Applicant was training one of the CWOs, who was the lead on the project. When the CWO saw the classified video, he told Applicant that it was prohibited to have this classified data on an unclassified company computer. Applicant testified that he was surprised and upset. The CWO told Applicant not to delete the images, but to be sure they were protected. Mr. C, a civilian contractor who also worked on the project and saw the images, told Applicant he should delete them. However, Applicant decided to follow the instructions of the CWO, and he knew the data was password protected, so he did not delete them. He testified, "I listened to the

uniformed chief warrant officer who was now the lead." Applicant brought his computer to his apartment in State A, because there had been thefts in the area where he was working. He did not contact his FSO after he was informed that he had committed a security violation. There is no record evidence that he stored the computer in an approved safe while he worked in State A. (GE 2; AE A, B; Tr. 110-117, 214-215, 219-220)

In early December 2007, Applicant informed his FSO that he would be out of the country from December 3 to December 14. He testified that at least part of his awareness that he was required to contact his FSO about foreign travel came from the General Security Briefing he received on his first day at Company B. He went on vacation to Asia with his parents. On December 6, Major A emailed Applicant asking him to call. However, Applicant did not have email access during his trip abroad. Also on December 6, Major A informed Applicant's manager and FSO at Company B that Applicant had committed a security violation by having classified images on his work computer. Between December 6 and December 12, Company B's FSO and senior-level personnel, pertinent military members, the Defense Security Service, and Naval Criminal Investigative Service (NCIS) personnel were notified of Applicant's security violation. (AE C-G; Tr. 111-116, 118, 248, 257-258)

When Applicant returned to work in State A on December 14, 2007 after his vacation, his supervisor told him that there had been potential security violations related to (1) Major A's use of the classified CDs; and (2) Applicant's downloading of classified images onto his work computer. The case was referred to NCIS for investigation. Applicant's apartment in State A was searched for classified data. On December 14, his computer and thumb drive were confiscated and provided to NCIS. Applicant gave a statement to an NCIS investigator on December 17, 2007. He then flew back to his home state and met with his manager, a human resources representative, a vice president, and the FSO. On December 18, Applicant gave a statement to the FSO. He was removed from the T&E project, prohibited from having contact with Major A, and was required to report any attempted contact by Major A. On December 19, 2007, Applicant forwarded to his FSO an email he received from Major A. (GE 2; AE H, I; Tr. 119-130)

In January 2008, Applicant returned to his original worksite and to his previous assignment of logistics analysis. The FSO gave him security briefings on how to handle and store classified data, and related material to read.[11] The FSO reported in the security database that, "Due to the circumstances and amount of time the information has been out there, it is felt that a compromise cannot be precluded." Company B

[11] GE 3, the NCIS report of investigative action, contains two pages related to guidance for couriers of classified material. Although the pages are not signed as received by Applicant, the date on the NCIS cover sheet indicates that Applicant received the courier briefing on December 17, 2007, which is after Applicant had couriered the classified information to Major A. Applicant testified that he received this information on courier requirements in January 2008. Whether he received the courier instructions in December 2007 or January 2008**,** I find that he did not receive the courier guidelines until after he had couriered the classified information in August 2007. (GE 3; Tr. 21-22, 87-88)

suspended Applicant for five days, and confiscated his badges and Common Access Card. Applicant does not believe that he was suspended, but only that he was told not to report to work for a week and to use his leave hours. Applicant's security clearance was suspended for six months. It was reinstated on July 28, 2008. In his August 2008 performance evaluation, Applicant was rated as "Meets Expectations" for two job objectives and "Below Expectation" in the third objective, Classified Data. The evaluation noted his "self-admitted mishandling of, unauthorized couriering and disclosure of classified (Secret) [program name] test-related files…." In November 2008, before leaving Company B, Applicant received a Certificate of Appreciation from his Department of Defense customer for his work. (GE 3, 4; AE J, V, W; Tr. 130-133, 165, 235-236)

The program manager for the Company B T&E team, who knew Applicant in 2008, describes him as task-oriented, ambitious, and mature for his age. Applicant's 2009 performance evaluation from his current employer notes that he is an outstanding asset to the customer, and he "meets and may exceed some goals." One of his customers, who has known him for one year, found him to be motivated, hard-working, and of good character. A friend-coworker describes him as being conscientious and having sound judgment. Another close friend-coworker opined that Applicant has integrity and reliability. Applicant's friend of nine years believes that it is not in Applicant's nature to violate rules and regulations. His current supervisor, who testified on his behalf, recommends Applicant as honest, trustworthy, and without guile, and someone who displays good judgment. Company B's FSO testified that Applicant did an excellent job as temporary FSO while the FSO was on medical leave. He considers Applicant to be honest, reliable, and responsible. (AE AA, X, Y, Z, BB, CC, DD; Tr. 157-158)

Policies

Each security clearance decision must be a fair, impartial, and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the revised AG.[12] Decisions must also reflect consideration of the "whole-person" factors listed in ¶ 2(a) of the Guidelines.

The presence or absence of disqualifying or mitigating conditions does not determine a conclusion for or against an applicant. However, specific applicable guidelines are followed whenever a case can be measured against them, as they represent policy guidance governing the grant or denial of access to classified information.

[12] Directive. 6.3.

A security clearance decision is intended only to resolve the question of whether it is clearly consistent with the national interest[13] for an applicant to receive or continue to have access to classified information. The Government bears the initial burden of producing admissible information on which it based the preliminary decision to deny or revoke a security clearance. Additionally, the Government must be able to prove controverted facts alleged in the SOR. If the Government meets its burden, it falls to applicants to refute, extenuate or mitigate the Government's case. Because no one has a "right" to a security clearance, applicants bear a heavy burden of persuasion.[14] A person who has access to classified information enters a fiduciary relationship based on trust and confidence. The Government has a compelling interest in ensuring that an applicant possesses the requisite judgment, reliability, and trustworthiness to protect the national interest as his or her own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access to classified information in favor of the Government.[15]

Analysis

Guideline K, Handling Protected Information

AG ¶ 33 expresses the security concern pertaining to handling protected information:

> 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 following disqualifying conditions under AG ¶ 34 are relevant to the facts of the case and raise a security concern:

> (b) collecting or storing classified or other protected information at home or in any other unauthorized location;
>
> (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

---

[13] *See Department of the Navy v. Egan*, 484 U.S. 518 (1988).

[14] *See Egan,* 484 U.S. at 528, 531.

[15] *See Egan;* Revised Adjudicative Guidelines, ¶ 2(b).

computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment;

(g) any failure to comply with rules for the protection of classified or other sensitive information; and

(i) failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent.

In August 2007, Applicant violated security rules by carrying classified CDs to the home of his supervisor, Major A. Applicant claims that he did not know this was a violation because he did not receive the courier guidelines until after he had couriered the CDs. In addition, the FSO did not alert Applicant to a security issue because she thought he was taking the CDs to the Major's office, i.e., that Applicant was carrying them from one cleared facility to another cleared facility. Applicant may not have realized at first that his couriering was a violation, although the Major's instructions not to tell anyone about it should have raised a flag.

However, *after* Applicant handed over the CDs, the Major explicitly told him that bringing the CDs to his house was wrong. At that point, Applicant knew or should have known that his couriering to a personal residence was a security violation. Despite this knowledge, he left the CDs at Major A's home. He did not determine if there was a safe to store the material; he did not obtain a receipt. He reported neither Major A's conduct nor his own to his FSO, as required by item 19 of the General Security Briefing that he signed. As cited in SOR allegation 1.c., his actions also violated the following NISPOM sections:

5-100. General. Contractors shall be responsible for safeguarding classified information in their custody or under their control. Individuals are responsible for safeguarding classified information entrusted to them. The extent of protection afforded classified information shall be sufficient to reasonably foreclose the possibility of its loss or compromise.

5-401. Preparation and Receipting
a. Classified information to be transmitted outside of a facility shall be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that CONFIDENTIAL information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, the addressee and the document, but shall contain no

classified information. It shall be signed by the recipient and returned to the sender.

5-410. Use of Couriers, Handcarriers, and Escorts. Contractors who designate cleared employees as couriers, handcarriers, and escorts shall ensure:…
c. The employee retains classified material in his or her personal possession at all times. Arrangements shall be made in advance of departure for overnight storage at a U.S. Government installation or at a cleared contractor's facility that has appropriate storage capability, if needed.

5-303. SECRET Storage. SECRET material shall be stored in a GSA-approved security container, an approved vault, or closed area.

Applicant subsequently downloaded classified information from the CDs onto his work computer, which was not approved for classified information. The data was stored on his computer for four months, until December 14, 2007. During that period, at times he brought his work computer home at night. At those times, his computer was not secure. He then traveled with the computer from his home state to his temporary duty in State A. He kept the computer at his worksite in State A. He also brought it to his apartment in State A after work hours. Nothing in the record indicates that Applicant followed security rules to protect the classified information on his computer during this extended period. The data was vulnerable to disclosure numerous times between August and December, until it was confiscated in December 2007. AG ¶ 34(b) and (c) apply. His actions also violated these NISPOM sections cited in SOR allegation 1.b.:

5-100 (*supra*)

8-100. General
a. Information systems (IS) that are used to capture, create, store, process or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information, loss of data integrity to ensure the availability of the data and system.
b. Protection requires a balanced approach including IS security features to include but not limited to, administrative, operational, physical, computer, communications, and personnel controls. Protective measures commensurate with the classification of the information, the threat, and the operational requirements associated with the environment of the IS are required.
c. The requirements outlined in the following sections apply to all information systems processing classified information. Additional requirements for high-risk systems and data are covered in the NISPOM Supplement.

8-105. Users of IS. Users of IS are either privileged or general users….
b. General users are individuals who can input information to or modify information on an IS or who can receive information from an IS without a reliable human review.
c. All users shall:
(1) Comply with the IS Security Program requirements.
(2) Be aware of and knowledgeable about their responsibilities in regard to IS security.
(3) Be accountable for their actions on an IS.
(4) Ensure that any authentication mechanisms (including passwords) issued for the control of their access to an IS are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access.
(5) Acknowledge, in writing, their responsibilities for the protection of the IS and classified information.

While the CDs were in Applicant's custody in his home state, he stored them in a container in his office at Site A. In his statement to the NCIS investigator, he said the container was a file cabinet that was not approved for storage of classified data. However, the FSO subsequently verified that the sole container in Applicant's office, which Applicant thought was not approved, was in fact a GSA-approved safe with an X09 lock that was aprroved to store secret data. Applicant's actions, as cited in SOR allegation 1.a., did not violate section 5-100 (*supra*) or 5-303 (*supra*), because in August 2007, in his office, he stored the secret data in an approved safe.[16]

Applicant admits his security violations, but claims that his employer did not train him in the handling of classified information. However, Applicant testified that he read and signed the General Security Briefing provided by his employer. The briefing included the requirements and prohibitions surrounding the handling of classified information. By signing the General Security Briefing in October 2006, Applicant acknowledged his security responsibilities, and was on notice that classified information was subject to those rules to prevent its disclosure. Applicant failed to follow these requirements. AG ¶ 34(g) applies.

AG ¶ 34(i) relates to damage to the national security as a result of failure to follow rules. The record does not contain sufficient evidence to show such damage. The FSO indicated only that compromise of the information could not be ruled out, given the extensive amount of time that Applicant failed to protect the classified information. AG 34(i) does not apply.

[16] There is no record evidence that Applicant kept his computer in an approved safe while he was at his work site in State A. Moreover, he testified that he usually took his computer to his apartment in State A after work. During those times, it was not secured in a safe. Applicant violated NISPOM sections 5-100 and 5-303 while in State A from September to December 2007. However, failure to store the data in a secure container during that period was not alleged in the SOR.

AG ¶ 35 provides conditions that could mitigate security concerns, including the following relevant conditions:

> (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;
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and,
>
> (c) the security violations were due to improper or inadequate training.

Applicant's actions did not occur under unusual circumstances, but rather in the regular course of his duties. He committed an ongoing security violation that began in August and continued until December 2007. Although the events occurred three years ago, the extent of the violation outweighs any claim that they are not recent. Each CD contained three videos and about 20 images. He downloaded eight CDs to his work computer, which resulted in storing 24 classified videos and approximately 160 images on his unclassified computer. This large volume of critical information regarding testing and evaluation of military equipment remained at risk until Applicant's computer was confiscated. His actions reflect poorly on his reliability and judgment, and AG ¶ 35(a) does not apply.

Applicant received security training at the Defense Security Service Academy, and functioned as the FSO while his current company's FSO was on sick leave. As a result, he has greater knowledge of security regulations than he did in 2007. In addition, the record shows that Applicant's company should have been more diligent in ensuring that Applicant had sufficient security training. While Applicant receives some mitigation under AG ¶ 35(b) and (c), it must be viewed in light of the scale of Applicant's conduct: He ignored the Major's plain statement that their actions were wrong; he downloaded classified information to an unauthorized computer; he left classified information unprotected for an extended period; and even after being told by the CWO and contractor that he had committed a security violation, he failed to inform his FSO or any other authority. The mitigation available under AG ¶ 35(b) and (c) does not outweigh the significance of Applicant's actions.

Guideline M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern related to use of information technology systems:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns

about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

AG ¶ 40 describes disqualifying conditions that could raise a security concern, including the following relevant conditions:

> (d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system; and
>
> (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations.

As discussed *supra*, Applicant inserted CDs with secret data into his work computer, which was not approved to store classified data. He then downloaded approximately 24 videos and 160 images of the testing of military equipment, and failed to properly protect it over an extended period. AG ¶ 40(d) and (f) apply.

AG ¶ 41 provides the following relevant mitigating conditions:

> (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of a supervisor.

Applicant's actions occurred during his routine work, not in unusual circumstances. Moreover, his conduct was not minor, as his actions placed secret defense-related information at risk. Although this conduct occurred several years ago, the importance of the data that was put at risk, and the length of time that passed before it was remedied, outweighs the distance in time. AG ¶ 41(a) does not apply.

Applicant downloaded the classified information after seeing Major A do it. Even if, *arguendo*, Applicant did not intend to violate security rules when he copied the CDs at his work site, his behavior after he transferred to State A shows that he was not acting in good faith. In State A, the CWO and Mr. C alerted him to the fact that he was

committing a security violation by having the classified data on his unclassified computer. But Applicant did not contact his FSO, or seek out an approved container in which to store the computer, or determine some appropriate way to protect the information. Instead, he brought the computer to his apartment in the evenings, where it was unprotected. Within days, he departed for a trip to Asia, leaving the computer in his apartment where it remained unprotected for an additional two weeks. AG ¶ 41(c) does not apply.

Guideline E, Personal Conduct

> AG ¶ 15 expresses the security concern pertaining to personal conduct:
>
> 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….

AG ¶ 16 describes conditions that could raise a security concern, including the following relevant condition:

> (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…

Applicant failed to follow security requirements that he knew or should have known after reading and signing the security briefing. His violations included transporting secret data to a private home; downloading that data onto an unclassified computer; and failing to store his computer containing classified data in an approved container when he was in State A. Even if, as he contends, he did not know these were violations, once the CWO pointed it out, Applicant still decided not to inform his FSO of his violations, still kept his computer with classified information in his apartment, and left for an overseas trip with the computer still unprotected. Applicant's conduct was highly untrustworthy, shows poor judgment, and demonstrates a willingness to ignore rules. AG ¶ 16(d) applies.

AG ¶ 17 provides conditions that could mitigate security concerns under Personal Conduct guideline. The following conditions are relevant:

> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and
>
> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

Applicant is now aware that he failed to follow important security regulations. He has taken security courses. He is qualified as an FSO and performed well when he acted as FSO on a temporary basis for his current employer. AG ¶ 17(d) applies. However, Applicant's violations of the security rules and regulations were frequent, as they extended over a period of four months. In addition, his violations were of the most serious type, as they involved exposing secret data to disclosure. Applicant failed to notify security officials of the possible compromise, and his own and the Major's violations, in August 2007. He again decided not to inform his FSO in November 2007, after he was specifically told he was in violation. AG ¶ 41(a) does not apply. The magnitude of Applicant's violations raises serious doubts about his reliability and judgment and outweighs the mitigation under AG ¶ 17(d).

Whole-Person Analysis

Under the whole-person concept, an administrative judge must evaluate an applicant's security eligibility by considering the totality of an applicant's conduct and all the relevant circumstances. An administrative judge should consider 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.

AG ¶ 2(c) requires that the ultimate determination of whether to grant a security clearance be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. Under the cited guidelines, I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case.

It is not credible that Applicant was unaware that his actions violated security rules. He is an intelligent and well-educated young man. Having read the security brief, and heard the Major's instruction not to tell anyone and his plain statement that what they were doing was wrong, Applicant knew or should have known that he had to, at the least, contact his FSO for guidance. He testified that he did not think the man who wrote the security protocols could be breaking the rules. But that man specifically stated to Applicant that they were breaking the rules, and certainly, the man who wrote the security protocols would be the one who would know they were breaking the rules.

Company B shares some responsibility: it should have been more thorough in providing security information to Applicant when he joined the company, and it should have presented the courier briefing to him before he transported classified material, not after. But Applicant had responsibilities as well. Once he read and signed the security brief, he was responsible for following the requirements. His signature is a valid and binding acknowledgment that he read the security requirements. To rule otherwise would render meaningless the certifications and acknowledgments that applicants sign.

Even if Applicant's actions in his home state were excused based on ignorance, he could not be excused for his conduct in State A. The CWO and Mr. C told him he had broken security rules by placing classified data on an unauthorized computer. Yet, with this knowledge that he had committed a serious security violation, and that classified information was at risk, he committed an additional violation by failing to inform his FSO of a possible compromise. Nor did he notify his supervisor or any authorized person. Although he knew that the classified CDs had to be stored in the locked safe at his office in his home state, he did not seek out an approved container in State A to store his computer, and he took his computer to his apartment during non-working hours. Finally, he left the computer in his apartment while he traveled overseas for two weeks.

Applicant's youth and inexperience at the time of these events explain his conduct to some extent, especially his failure to report Major A, a powerful person whom Applicant did not feel comfortable challenging. But this failure shows a serious lack of judgment. The Government must be able to rely on those who hold security clearances to place the Government's interests above their own. In addition, Applicant's failure to inform the FSO, once he was told he was in violation, was a conscious decision to violate security regulations. His actions not only raise questions as to his trustworthiness, but are particularly troubling because they violate the regulations on which the industrial security system is based.

Overall, the record evidence fails to satisfy the doubts raised about Applicant's suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the security concerns arising from the cited adjudicative guidelines.

Formal Findings

Paragraph 1, Guideline K	AGAINST Applicant
Subparagraph 1.a.	For Applicant
Subparagraph 1.b. – 1.c.:	Against Applicant
Paragraph 2, Guideline E	AGAINST Applicant
Subparagraph 2.a.	Against Applicant
Paragraph 3, Guideline M	AGAINST Applicant
Subparagraph 3.a.	Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the interests of national security to allow Applicant access to classified information. Applicant's request for a security clearance is denied.

RITA C. O'BRIEN
Administrative Judge