**DEPARTMENT OF DEFENSE**
**DEFENSE OFFICE OF HEARINGS AND APPEALS**

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| | ) | ISCR Case No. 13-00676 |
| | ) | |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Robert J. Kilmartin, Esquire, Department Counsel
For Applicant: *Pro se*

03/24/2014

## Decision

MATCHINSKI, Elizabeth M., Administrative Judge:

Applicant is an engineer with a record of four security violations. He left a classified tape on a bench in a laboratory in November 2006. In June 2012, he failed to secure a lock on a classified closed area. In October 2012, he left six classified hard drives unsecured in a closed area that was secured but not approved for open storage. In December 2012, he installed unapproved software on a classified information system. Applicant has since established routines to remind him of his security responsibilities, but his negligence in fulfilling his security responsibilities continues to cast doubt about his security worthiness. Clearance denied.

## Statement of the Case

On August 23, 2013, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline K, Handling Protected Information, and explaining why it was unable to find it clearly consistent with the national interest to grant or continue a security clearance for him. The DOD CAF took the action 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) effective within the DOD on September 1, 2006.

Applicant responded to the SOR allegations on September 6, 2013, and on September 12, 2013. He requested a hearing before a Defense Office of Hearings and Appeals (DOHA) administrative judge, and on January 14, 2014, the case was assigned to me to conduct a hearing to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for him. On January 17, 2014, I scheduled a hearing for February 11, 2014.

I convened the hearing as scheduled. Three Government exhibits (GEs 1-3) and three Applicant exhibits (AEs A-C) were admitted into evidence without objection. Applicant also testified, as reflected in a transcript (Tr.) received on February 20, 2014. At the Government's request and with Applicant's agreement, the SOR was amended to conform to the evidence. SOR 1.a was amended to correctly reflect where the incident occurred. SOR 1.b was amended to indicate that Applicant failed to secure the lock on the door to a classified laboratory.

On February 21, 2014, I took action to reopen the record for Applicant to clarify his hearing testimony indicating that he may have performed classified work after his security clearance had been suspended by the DOD. Applicant's response of March 5, 2014, was admitted as a hearing exhibit (HE 1) without objection.

## Findings of Fact

The amended SOR alleges under Guideline K that Applicant committed four security violations while working for his current employer in a classified laboratory.[1] Specifically, in November 2006, he left a classified backup tape on a bench in the laboratory (SOR 1.a). In June 2012, he failed to secure the lock on the door to the classified laboratory (SOR 1.b). In October 2012, he left six, Secret-classified hard drives in the closed area overnight without properly storing them in an approved storage container (SOR 1.c). Then, in December 2012, he installed unapproved software on a classified information system (SOR 1.d). Applicant does not contest that his conduct was in violation of the rules and regulations for protecting classified information, although he denies any deliberate noncompliance. After considering the pleadings, exhibits, and transcript, I make the following findings of fact.

[1] The SOR placed Applicant on notice of the conduct of security concern under Guideline K, but not of the security regulation, practice, or procedure that he allegedly violated by his conduct. At the hearing, Department Counsel similarly did not cite to the National Industrial Security Program Operating Manual (NISPOM) or any security procedures of Applicant's employer implementing the provisions of the NISPOM. Applicant does not contest that he committed the conduct alleged or that he thereby violated the rules and regulations for protecting classified information. Consistent with my obligation as the finder of fact, I reviewed the NISPOM to determine whether Applicant in fact violated any security requirements.

Applicant is a 32-year-old, married electrical engineer with two young children. He holds a master's degree awarded to him in January 2011. He earned his undergraduate degree in May 2004. From July 2004 to November 2005, he was employed as a research engineer for a defense contractor. He was granted a Secret clearance for his duties with that company in June 2005. (Tr. 27.) In December 2005, Applicant went to work for his current defense contractor employer, as a member of its technical staff. His Secret clearance eligibility was transferred for his current employment. (GE 1.)

Applicant's work required access to a closed area computer laboratory approved for classified work to the Secret level but not approved for open storage of classified material (e.g., hard drives, tape drives, backup tapes, and documents). (GE 3; Tr. 23, 26.) Applicant received security briefings on the company's classified information system and classified computer laboratory, which included proper conduct in the lab and the protection of classified information. (Tr. 28.) Applicant also received annual security awareness refresher briefings, primarily consisting of Power Point presentations advising employees of the security procedures they are to follow. (Tr. 40.)

Around November 2006, Applicant left a classified backup tape unsecured on a bench in the computer laboratory. The computer lab itself was properly secured by lock (X-09 cipher lock) and alarm, and Applicant presumed that the lab had been approved for open storage of classified information. (Tr. 26.) Applicant was disciplined by his employer for not securing the tape in an approved storage container within the computer lab. (GE 1.)

Starting around 2011, Applicant became the lead hardware engineer and senior systems integration engineer on a program where he has had to work independently, often as the only engineer in his office assigned to the program. His duties included the development, debugging, and testing of hardware and firmware, primarily in the classified secure environment of the closed area computer lab. Applicant worked closely with the security staff at his facility to coordinate the classified development environment for the program. (AE A.)

On June 29, 2012, Applicant forgot to spin the X-09 dial lock on the door to computer lab. (GEs 1-3; Tr. 35-36.) Applicant speculates that he was focused on the project at hand. It was a stressful time for him in that there were design issues to work through, which required him to access the lab several times a day. (Tr. 23, 29.) Whereas the computer lab was alarmed and secured by a card reader, his employer determined there was no compromise or loss of classified material. (GEs 1-3.) Applicant was given a refresher briefing for closed area procedures by his employer in July 2012 because of this security violation. (GE 3.) The facility security officer (FSO) implemented a program requiring each employee with access to the computer laboratory to wear a red badge reminding him or her of the procedures to open and close the lab. (Tr. 23-24.)

Applicant completed annual security refresher training in August 2012. (GE 3.) In mid-October 2012, he left six hard drives unsecured on a bench in the closed area overnight. Applicant indicates that the drives did not contain classified data, but he admits that they should have been protected as Secret information. (GE 1.) In reporting the infraction, his employer indicated that the hard drives were classified Secret. (GE 3.) The closed area was secured by lock and alarm, but the hard drives were not in an approved storage container. (GEs 1-3.) Applicant's employer determined that there had been no loss or compromise of classified information, but Applicant received a written reprimand and information systems refresher training in October 2012 for his second security violation. (GE 3; Tr. 32.) Applicant believes that the incident likely happened when he was leaving work late at night, and he "needed to get home." He failed to see the drives on the lab bench while he was busy securing everything else in the lab. (Tr. 24.)

In December 2012, Applicant installed unapproved compact disk (CD) burner software on a classified information system at work. He obtained the software from the Internet.[2] He assumed that there was no problem with installing the software because he had seen the software on unclassified work stations. (Tr. 25, 39.) Applicant made no effort to check with security or information technology personnel about whether the software was authorized for use on a classified information system. (GEs 1-3; Tr. 25.) No compromise or loss of classified material occurred, but because of Applicant's pattern of three security violations since late June 2012, his employer submitted an individual culpability report to the DOD on January 2, 2013. (GE 3.) In response to the incident, Applicant printed a list of the rules pertaining to classified information systems and posted it in the lab as a reminder of what constitutes acceptable use of the information system. (Tr. 39.) After the security infraction, Applicant continued to work in the classified lab. He obtained an escort for him to enter the lab, but the escort otherwise left him to perform his classified work until he needed the exit the lab. The escort would then ensure that he properly secured the lab. (Tr. 31-32.)

[2] When asked to explain why he thought it was okay to install software obtained from the Internet when he could not guarantee its security, Applicant responded:

> Well, I understand the concern, but a lot of the software that we use is obtained through the Internet, you know, simple software that's used. Like, for example, Adobe Reader, that's obtained from the Internet and we use that on all our classified PCs. I believe the Microsoft Office Suite, I think you can get that through hard CDs, but at some point the hard CDs, I think you can install updates from the Internet, so a lot of our software is used and it's okay to do that. You just have to make sure that you let them know, let them know your intent and say, hey, I got this software, this is what I want to do with it. And then they basically bless it and say it's okay to do that . . . After that incident, I do remember my FSO, she wasn't quick to call this a violation. She wanted to make sure that our headquarters in [state name omitted] that this was an approved [software] and that news just hadn't made it to our office yet. So she actually did check and the person who she spoke to actually did say—she named the name of the software and the guy said, oh, this is—this is approved software, but let me double check. And it turned out, after some research, that it was not in fact approved, but I think that shows that this software was used widely at [employer omitted]. It just hadn't crossed that threshold into approved software yet. (Tr. 37-38.)

On January 28, 2013, Applicant completed and certified to the accuracy of an Electronic Questionnaire for Investigations Processing (e-QIP). Applicant disclosed his four security violations since November 2006 in response to whether, in the last seven years, he had received a written warning, been officially reprimanded, been suspended, or been disciplined for misconduct in the work place, including for a violation of security policy. Applicant also answered "Yes" to the following:

> **In the last seven (7) years** have you introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations or attempted any of the above?

Applicant explained that he received a written reprimand from his FSO for installing "CD burner SW that is used on unclassified systems at [employer], but wasn't yet approved for classified systems." (GE 1.) Applicant submits that the new procedures in the laboratory, which include the wearing of a lanyard with reminders of one's security responsibilities, have helped him maintain security compliance. (Tr. 25.)

On March 7, 2013, Applicant was interviewed by an authorized investigator for the Office of Personnel Management (OPM), partially about his security violations in 2012. Concerning the incident in June 2012, Applicant admitted that he neglected to spin the lock to a neutral position on the door to the computer laboratory, although he had armed the alarm. A co-worker, who opened the laboratory the next day, discovered the violation and reported it to security. Applicant also admitted that he received a written warning from security after he left six hard drives on a bench in the computer lab in October 2012. He "just forgot" to secure the hard drives before he left the lab that day. As for the December 2012 violation, Applicant had downloaded CD burner software obtained from an unsecured Internet site onto a work computer "to complete a trusted download briefing for work." He transferred the software to a CD that he then used to install the software to a classified workstation. Applicant denied knowing that the software was not approved because he had seen the program on other workstations. He admitted that he had not consulted with security at work before inputting the CD. (GE 2.)

In April 2013, the DOD suspended Applicant's security clearance eligibility because of his violations of security procedures in 2012. (Tr. 43.) He was reassigned to a program that does not require a security clearance, but he also testified that he was "able to do classified work with somebody else on [his] program." He also indicated that he "accessed classified systems." (Tr. 41-42.) In response to my post-hearing request for clarification, Applicant explained that on about 50 occasions after his clearance was suspended, he was allowed to continue to work in the classified laboratory, but only when accompanied by a cleared escort, who alerted those employees working on classified materials to the presence of an uncleared individual. Applicant did not view any classified material. He accessed classified work stations to program and debug a product using standard software tools that did not visually display classified

information.[3] On occasion, he needed to operate the software tools to view debugging information or program the product if it was not operating correctly, "simply because [he is] more of a subject matter expert on the product than [his] escort." Applicant's understanding was that he could not access any classified documents on screens, but accessing classified hardware (product, programming cables, and hard drives) was acceptable with an escort because the classified hardware was not visually classified. (HE 1.)

Reinstatement of Applicant's security eligibility is endorsed by the general manager/vice president of his company's local operations (AE C); by the onsite supervisor tasked with issuing Applicant's performance reviews while not directly overseeing Applicant's work (AE B); and by the senior program manager for a family of encryption products, who interacts with Applicant long distance (AE A.) Applicant has shown his general manager that he understands his responsibilities associated with working with classified programs. This manager considers Applicant an asset and he would not hesitate to hire him again to support such programs. (AE C.) The onsite supervisor has known Applicant since 2005, when they both started with the company. Applicant has demonstrated dedication and focus at work, such that he is regularly praised "for both his attention to details as well as his ability to keep big picture ideas in perspective." This supervisor is aware of the three security incidents. He was surprised by the June 2012 infraction and considered it uncharacteristic of Applicant's attention to detail. Following the third incident, Applicant impressed the supervisor with his commitment to establishing new routines to ensure there would be no future infractions. In hindsight, the supervisor considers it "disappointing" that Applicant did not take similar measures after the second infraction, but he is convinced that Applicant can be trusted with access to sensitive information. "[Applicant's] dedication to fixing mistakes and his determined, focused mentality will help him be vigilant against any future incidents." (AE B.)

## Policies

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

[3] Applicant explained his access to classified work stations as follows:

> They did not allow me to view classified material after my clearance was suspended. However, to continue with my debugging work in the classified lab, our product needed to be opened (cover removed) to allow access to test connectors. This alone makes the product classified, but it is not visually classified. Classified debug software images needed to be programmed into the product from the workstation. However, what makes them classified is that they are not encrypted. I did not view any classified source code. The programming tool does not show any classified information. The programming cables are connected to the classified workstation and are therefore marked classified, but again not visually classified. Finally, debugging required hard drives that were marked classified since they were connected to our open (now classified) product. No classified data was actually stored on the hard drive. (HE 1.)

security clearance, the administrative judge must consider the adjudicative guidelines. 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 overall 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. 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 to obtain 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 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

### Guideline K, Handling Protected Information

The security concern for Handling Protected Information is articulated in 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 evidence establishes that Applicant committed four security infractions after he started with his current employer in December 2005. In November 2006 and again in October 2012, he left classified material unsecured in the computer lab overnight. As of February 28, 2006, the NISPOM (DOD 5220.22-M, ¶ 5-303) mandated supplemental controls, such as a safe, steel file cabinet or safe-type steel file container with an automatic unit locking mechanism, or a steel file cabinet secured by a rigid metal lock bar and an approved key operated or combination padlock, for the storage of Secret material in closed areas. Even if Applicant believed in good faith that classified information could be left in the open in a properly secured closed area in November 2006, he was disciplined by his employer for the infraction. Therefore, he knew as of October 2012 that the information on the hard drives had to be protected to the level of Secret before he left the computer lab. He violated ¶ 5-100 of the NISPOM, which clearly states that individuals are responsible for safeguarding classified information entrusted to them. In June 2012, Applicant failed to properly secure the computer lab by failing to spin the X-09 lock, so although he had armed the alarm, the closed area was not fully secured. He violated ¶ 5-306 of the NISPOM in that during non-working hours and during working hours when a closed area is unattended, admittance is to be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. Then, in December 2012, Applicant violated his responsibilities under ¶ 8-105 of the NISPOM as a user of a classified information system. He failed to ensure the integrity of a classified information system when he downloaded onto the classified system software obtained from an unsecure Internet site without authorization. Three disqualifying conditions under AG ¶ 34 are implicated:

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

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

(h) negligence or lax security habits that persist despite counseling by management.

AG ¶ 34(b) applies in that the classified lab was not approved for open storage, so the classified backup tape in November 2006 and the six Secret hard drives in October 2012 were found in an unauthorized location. AG ¶ 34(g) applies in that he failed to protect classified information, and in the case of the unapproved introduction of software, a classified information system. AG ¶ 34(h) is shown by his pattern of three security infractions within six months in 2012.

Under AG ¶ 35, Applicant's failure to fully comply with the rules and regulations for protecting classified information could be mitigated by the following:

(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.

Two of the violations (the November 2006 and October 2012 security incidents) were similar in that they involved the improper storage of classified information. The recurrence and recency of his security infractions preclude favorable consideration of AG ¶ 35(a). Concerning AG ¶ 35(b), it is difficult to conclude that Applicant responded favorably to remedial security training, given that the October 2012 improper storage of classified material and the December 2012 loading of unapproved software onto a classified system occurred after he received security refresher training, including his annual refresher briefing in August 2012.

Applicant has posted the rules for protecting classified information systems and the classified laboratory in his work area, and he wears the lanyard established by his employer to remind him of his security responsibilities. Applicant's improved focus on security measures, which has been observed by an onsite manager, do not fully mitigate the security concerns, especially those raised by his downloading of unapproved software from the Internet onto a classified network. Applicant made assumptions inconsistent with his security obligations. Applicant testified that he now realizes that he has to check with his FSO first to see whether he can install software on a classified system (Tr. 25), but concerns persist that he lacks appropriate security awareness. Applicant testified that he was allowed to perform classified work after his clearance was suspended by the DOD in April 2013, provided he was escorted. When asked about this potentially unauthorized access, Applicant responded, "I think they deemed it okay, I guess, maybe because this was pending investigation." He admitted he did not know whether the practice was consistent with the NISPOM (Tr. 41), and he apparently took no steps on his own to determine whether his work was security compliant. Applicant clarified after the hearing that his "classified work" involved escorted access to classified hardware that was not visually classified. He operated software tools to view debugging information or to program the product "simply because [he is] more of a subject matter expert on the product than [his] escort." (HE 1.) Assuming Applicant's work was not classified,[4] he should have recognized that describing his work as classified to the Government in February 2014 was inappropriate and could raise security flags.

[4]*See* ¶ 8-304 of the NISPOM, which authorizes maintenance by uncleared personnel with an appropriately cleared and technically qualified escort who monitors and records the activities of the uncleared person in a maintenance log.

Concerning AG ¶ 35(c), Applicant has not blamed his violations on inadequate security training. The June 2012 and October 2012 violations are attributable to Applicant being so focused on his work that he failed to pay due attention to his security responsibilities. The December 2012 infraction was due to Applicant not realizing the potential security risks of installing software from an unsecured Internet site onto a classified network. By that time, Applicant had worked primarily in a classified environment for seven years and could reasonably be expected to have understood that classified systems have different security requirements than non-classified systems. At a minimum, he should have checked with security or information technology personnel about whether the software could safely be downloaded in the classified environment. AG ¶ 35(c) does not apply.

**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).[5]

Applicant did not set out to circumvent security regulations. Yet, three security violations in six months in 2012 casts serious doubt about his judgment and reliability with regard to the handling of classified information. Applicant's onsite manager has been impressed by Applicant's renewed commitment to executing his security responsibilities perfectly since then, and he recommends reinstatement of Applicant's security clearance. Should Applicant's clearance be reinstated, he may well resume his classified duties, which have often required that he work independently and without direct oversight. The Government must be assured that he possesses the security knowledge and awareness to recognize any potential security issue so that he can seek security guidance if appropriate. His evidence falls short in this regard. It is well settled that once a concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against the grant or renewal of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990). Based on the facts and circumstances before me, I do not find it clearly consistent with the national interest to reinstate Applicant's security clearance eligibility at this time.

[5] The factors under AG ¶ 2(a) are as follows:

> (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.

## Formal Findings

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

| | |
|---|---|
| Paragraph 1, Guideline K: | AGAINST APPLICANT |
| Subparagraph 1.a: | Against Applicant |
| Subparagraph 1.b: | Against Applicant |
| Subparagraph 1.c: | Against Applicant |
| Subparagraph 1.d: | Against 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 or continue Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

Elizabeth M. Matchinski
Administrative Judge