KEYWORD: Security Violations; Personal Conduct

DIGEST: Applicant was cited for three security violations, one in 1996, and two in 2000. When balanced against the actions he has taken in response to those violations and his lengthy military and civilian careers during which he held a clearance without other incidents, the security concerns about his violations and personal conduct are mitigated. Clearance is granted.

CASENO: 04-01625.h1

DATE: 03/07/2006

DATE: March 7, 2006

In Re:

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

Applicant for Security Clearance

ISCR Case No. 04-01625

DECISION OF ADMINISTRATIVE JUDGE

MATTHEW E. MALONE

APPEARANCES

FOR GOVERNMENT

Ray T. Blank, Esquire, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant was cited for three security violations, one in 1996, and two in 2000. When balanced against the actions he has taken in response to those violations and his lengthy military and civilian careers during which he held a clearance without other incidents, the security concerns about his violations and personal conduct are mitigated. Clearance is granted.

STATEMENT OF THE CASE

After reviewing the results of Applicant's background investigation, adjudicators for the Defense Office of Hearings and Appeals (DOHA) were unable to make a preliminary affirmative finding[(1)] it is clearly consistent with the national interest to give Applicant a security clearance. On March 14, 2005, DOHA issued to Applicant a Statement of Reasons (SOR) alleging facts that raise security concerns addressed in the Directive under Guideline K (security violations) and Guideline E (personal conduct). Applicant timely answered the SOR, and requested a hearing.

The case was assigned to me on September 9, 2005, and I convened a hearing October 20, 2005. The parties appeared as scheduled and the government presented six exhibits (GE 1 through 6), which were admitted without objection. Applicant and two other witnesses testified, and Applicant submitted one document admitted without objection as Applicant's Exhibit (AE) A. DOHA received the transcript (Tr) on November 1, 2005.

FINDINGS OF FACT

After a thorough review of the pleadings, transcript, and exhibits, I make the following essential findings of fact:

Applicant is 64 years old and has held his current job with a defense contractor since November 2001. Before this he worked for another defense contractor from September 1990 until October 2001. Applicant served in the United States

Navy from 1962, when he matriculated at the U.S. Naval Academy, until 1990, when he retired as a commander (paygrade O-5) after 26 years of honorable service as a commissioned officer in the surface warfare community. Applicant developed expertise in anti-submarine warfare (ASW) while in the Navy, and his assignments later in his career used that expertise on unified command staffs where he also worked with NATO counterparts. Applicant was first granted a security clearance while still at the Naval Academy in 1962, and he has held a clearance at various levels, including TS/SCI, ever since.

After retiring, Applicant went to work for a company that supported the planning and execution of Navy ASW exercises, often in overseas locations and in conjunction with allied naval forces. Applicant and his fellow employees worked in the same office space as their Navy customers. The spaces used were configured as open cubicle workstations for each person and were in a secure location intended to store and receive classified information as required. Telephone conversations involving classified information were to be carried out using a Secure Telephone Unit (STU-III). The STU-III is a telephone that can be used like any regular telephone for unclassified discussions. It also has been modified for encryption of voice conversations using keys turned at each end of the line when the parties determine they will be discussing classified information. While working for this employer, there were not enough STU-IIIs available for unplanned use. They were either broken or were reserved for use by the uniformed Navy members on staff.

On October 16, 1996, Applicant was involved in the planning of an ASW exercise to be held overseas. He received a phone call initiated by a Naval officer who was Applicant's counterpart in the overseas exercise area several time zones ahead of Applicant's east coast location in the U.S. During their conversation, the counterpart unexpectedly began discussing topics that Applicant was concerned were classified. Because of the time difference between the two sites, Applicant's counterpart wanted to complete their business before the end of his duty day. Applicant was not on a STU-III and none was immediately available. Applicant tried to talk around the information to avoid disclosing classified information but knew at the end of the conversation he had been unsuccessful. When he hung up, Applicant loudly expressed his frustration aloud at having to discuss classified information over a non-secure line because the Navy could not more readily provide a STU-III. Applicant's statement was heard by a member of the Navy inspection team evaluating the security posture of the organization Applicant's company was supporting. As a result of what was determined to be a security violation, Applicant was suspended without pay for two days.

The relationship between the company Applicant worked for and the Navy staff they supported was not ideal. There was tension between the civilian and military staffs, and Applicant's employer was concerned that the Navy was not happy with the support they were receiving and may look elsewhere for contractor support. When the aforementioned telephone conversation took place, the Navy command was also undergoing a periodic security readiness inspection. Discrepancies from whatever source - civilian or military - would reflect adversely on the officer-in-charge of that activity.

On Sunday, March 19, 2000, Applicant traveled overseas to a Naval command to conduct one of the aforementioned ASW exercises. He flew to a major city north of the command, arriving the morning of Monday, March 20, and rented a car to drive the remaining two hours to his destination. He had in his possession properly wrapped confidential exercise materials consisting of working papers and charts at the confidential level. Applicant was authorized to carry them from the U.S. Along the way he stopped for gas. When he went inside to pay, his car containing all his possessions and the exercise materials was stolen. He estimates he was less than 20 feet away from his car for no more than two minutes. He immediately notified all appropriate Navy officials, including the Naval Criminal Investigative Service (NCIS), his

employer, and local law enforcement personnel about what happened. He also took every available corrective action to ensure the exercise was not delayed or compromised in any way.

During the course of the investigation into the loss of classified materials when Applicant's car was stolen, it was determined he had possessed the materials at his home from the time he left work Friday, March 17, until he departed on travel Sunday, March 19. Applicant was an authorized courier of the materials in question, but it was determined he committed a security violation by keeping them at his home, which was not an authorized storage facility.

No adverse action was taken against Applicant as a result of the March 2000 events, but his company duly reported them to the Defense Security Service (DSS) as required by the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, January 1995. Neither DSS nor the Navy determined that Applicant's actions resulted in actual compromise of the information at issue. The information lost when the car was stolen was double wrapped and sealed as it had been when he left work the previous Friday and as required by Navy procedures at the time.

Since moving to his current job in 2001, Applicant does not travel as extensively as before and he does not carry classified material as part of his current duties. He supports a joint command and sometimes interacts with foreign military liaisons, but he is no longer an exercise planner per se. Applicant's violations discussed above are the only such incidents in an otherwise unblemished 43-year record of service in the military and civilian defense communities.

Two co-workers testified in support of Applicant. One was a retired Navy officer with more than 22 years enlisted and commissioned service, who also worked with Applicant in 1996 and 2000 when Applicant was cited for the aforementioned security violations. Notwithstanding those events, he recommended Applicant keep his clearance and spoke enthusiastically about Applicant's judgment, reliability, and dedication to the work his company does for the U.S. military. This witness also testified that Applicant is committed to following required security procedures and is keenly aware of the importance of sound practices in protecting classified information. Applicant's other witness retired from the military in 2000 as a Navy Force Master Chief, the highest enlisted rank in the service. He then went to work for a defense contractor also doing business at the same site as Applicant's employer. He has been Applicant's team leader since 2002, and, based on 26 years experience as a Navy cryptologist and his close observation of Applicant's work and his overall conduct, commended Applicant for his expertise, reliability, and judgment. He, too, spoke highly of Applicant's commitment to the need to properly safeguard classified material.

POLICIES AND BURDEN OF PROOF

A security clearance decision is intended to resolve whether it is clearly consistent with the national interest[(2)] for an applicant to either 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 for an applicant. Additionally, the government must be able to prove controverted facts alleged in the SOR. If the government meets its burden, it establishes that it is not clearly consistent with the national interest for an applicant to have access to classified information. The applicant must then present sufficient evidence 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 to comply with the government's compelling interest in ensuring each applicant possesses the requisite judgement, reliability and trustworthiness of one who will protect the national interests as his or her own.[(3)] The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the government.[(4)]

The Directive sets forth adjudicative guidelines[(5)] for consideration when evaluating an applicant's suitability for access to classified information. Security clearance decisions must reflect consideration of disqualifying and mitigating conditions listed under each adjudicative guideline as may be applicable to the facts and circumstances of each case. Each decision must also reflect a fair and impartial common sense consideration of the factors listed in Section 6.3 of the Directive. The presence or absence of a disqualifying or mitigating condition is not determinative of a conclusion for or against an applicant. However, specific applicable guidelines should be followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified information. Having considered the record evidence as a whole, I conclude the relevant adjudicative guidelines to be applied here are Guideline E (personal conduct) and Guideline K (security violations).

CONCLUSIONS

The government alleged Applicant committed three security violations, one in 1996 involving discussion of classified information over a non-secure line (SOR ¶ 1.a), one in March 2000 when Applicant improperly kept classified materials in his home en route to an overseas exercise (SOR ¶ 1.b), and one in March 2000 involving loss of classified materials when Applicant's car was stolen overseas (SOR ¶ 1.c). As addressed through Guideline K, a security concern exists when it is shown a person does not comply with security regulations. Such conduct raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Included in the SOR allegations are cites to specific sections of the NISPOM, which provides guidance, regulations, and requirements for proper handling of classified information in an industrial security context. Specifically, SOR ¶ 1.a alleges Applicant's actions violated NISPOM 5-100, 5-101, and 5-404. SOR ¶ 1.b alleges violations of NISPOM 5-100 and 5-304. SOR ¶ 1.c alleges violations of NISPOM 5-100 and 5-410.c. NISPOM 5-100 is a general requirement that defense contractors are responsible for any classified information in their charge. NISPOM 5-101 prohibits discussion of classified information over unsecured telephones. NISPOM 5-304 requires materials classified as confidential to be stored the same as secret and to secret materials. NISPOM 5-404 requires that "transmission" of any confidential material outside a secure facility shall be done in the same way as secret material, but also allows confidential material may be sent by U.S. Postal Certified Mail. NISPOM 5-410.c provides that if a cleared contractor hand carries confidential materials outside a secure facility, he shall retain possession of that material at all times. Further, the contractor shall make arrangements in advance at an approved facility for any overnight storage that may be necessary.

Department Counsel has presented sufficient information to support the facts alleged in SOR ¶ 1. Those facts also constitute violations of the NISPOM provisions listed above. Available information supports the preliminary decision under Guideline K to deny Applicant's request to renew his clearance. Specifically, this record supports application of Guideline K disqualifying condition (DC) 1[(6)] and DC 2.[(7)] As to DC 1, Applicant discussed classified information over a non-secure telephone in October 1996. DC 2 applies to the October 1996 violation, in that Applicant was negligent by not insisting the other party to the phone call stop talking and make arrangements to continue the conversation on s secure phone. DC 2 applies also to the March 2000 violation wherein he took classified materials home the day before he flew overseas. This he knew at the time was not authorized, but was done as a matter of convenience. As to the arch 2000 violation resulting from the theft of his rental car overseas, some negligence may be assigned to Applicant in that he left the car unattended for a minute or two. However, it has not been shown the theft was a reasonably foreseeable event. Nonetheless, classified material was theoretically disclosed without authorization and both DC 1 and DC 2 must be considered here as well.

By contrast, Guideline K mitigating condition (MC) 1,[(8)] MC 2,[(9)] and MC 4[(10)] also apply to these facts. In considering application of MC 1, I conclude the October 1996 telephone discussion and the loss of the materials in March 2000 when his car was stolen were both inadvertent. As to the former, the call was originated by the other party, who was anxious to complete his business and who, without warning to Applicant, injected classified information into the conversation. Applicant was placed in the untenable position of having to stop the conversation to arrange for use of a STU III that he knew was unavailable anyway. Regarding the stolen car incident, it can be argued he should have been more attentive, however, such an event is unexpected, to say the least. This is not a case of Applicant leaving the materials wholly unguarded and out of sight while he attended to personal business. He was less than 20 feet away from the car for less than two minutes. He was otherwise in control of the materials at all times.

As to MC 2, these three events constitute the only errors of this kind in Applicant's Navy and civilian careers, which span more than 40 years. In his previous defense contractor job, he traveled extensively overseas, often carrying classified materials with him in much the same fashion as at issue here. All of these trips occurred without incident. MC 4 is applicable to the stolen car event because Applicant took significant corrective measures to eradicate any adverse impacts on the exercise for which the lost materials were to be used, and he made all possible notifications to the appropriate authorities. Regarding the 1996 telephone violation, Applicant put himself on report when he vented aloud his frustration at not having the resources needed to adhere to proper procedures. Further, co-workers with a wealth of experience in matters such as this have strongly recommended Applicant keep his clearance despite knowing that these three violations are in his background. In light of all available information on this issue, Applicant is not likely to commit future violations and can be relied on to abide by any and all procedures intended for the protection of classified materials. Accordingly, I conclude Guideline K for the Applicant.

The government has also expressed concerns, based on these same facts, about Applicant's judgment and reliability (SOR ¶ 2.a). Under Guideline E, a security concern arises where it is shown an applicant has exhibited questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations. Such conduct may indicate the person may not properly safeguard classified information.[(11)] The record evidence shows Applicant was involved in three security violations. However, as discussed above, only one violation involved any initiative by Applicant. He took classified information home with him as a matter of convenience when he traveled overseas. Of the listed disqualifying conditions under this guideline, only DC 5[(12)] warrants consideration based on these facts. However, for the same reasons I concluded under Guideline K that the violations in this case were

infrequent, I also conclude they do not constitute any pattern of rules violations. While the government may be generally concerned about Applicant's judgment because of the three incidents in Applicant's background, there are no specific disqualifying conditions applicable here. For the same reasons discussed under Guideline K, above, I conclude Guideline E for the Applicant.

A fair and commonsense assessment[(13)] of the entire record before me shows the government properly expressed reasonable doubts about Applicant's suitability to have access to classified information. The SOR was based on sufficient, reliable information about three security violations attributable to Applicant. Such issues bear directly on an applicant's ability to protect classified information, and to exercise the requisite good judgment and discretion expected of one in whom the government entrusts its interests. However, when considered in light of the entire record, the inadvertent and infrequent nature of these events, the fact the last violation occurred nearly six years ago, and Applicant's long history of properly safeguarding classified information in a variety of circumstances are sufficient to mitigate the security concerns expressed in this SOR. Available information shows it is clearly consistent with the national interest to continue Applicant's access to classified information.

FORMAL FINDINGS

Formal findings regarding each SOR allegation are as follows:

Paragraph 1, Guideline K (Security Violations): FOR THE APPLICANT

Subparagraph 1.a: For the Applicant

Subparagraph 1.b: For the Applicant

Subparagraph 1.c: For the Applicant

Paragraph 2, Guideline E (Personal Conduct): FOR THE APPLICANT

Subparagraph 2.a: For the Applicant

DECISION

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

Matthew E. Malone

Administrative Judge

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

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

3. *See Egan,* 484 U.S. at 528, 531.

4. *See Egan;* Directive E2.2.2.

5. Directive, Enclosure 2.

6. Directive, E2.A11.1.2.1. Unauthorized disclosure of classified information.

7. Directive, E2.A11.1.2.2. Violations that are deliberate or multiple or due to negligence.

8. Directive, E2.A11.1.3.1. Were inadvertent.

9. Directive, E2.A11.1.3.2. Were isolated or infrequent.

10. Directive, E2.A11.1.3.4. Demonstrate a positive attitude towards the discharge of security responsibilities.

11. Directive, E2.A5.1.1.

12. Directive, E2.A5.1.2.5. A *pattern* of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency. (emphasis added)

13. Directive, E2.2.3.