KEYWORD: Security Violations

DIGEST: Applicant, with an otherwise unblemished record of protecting and safeguarding classified information, committed a deliberate security violation by downloading unclassified files from his facility's classified computer onto his pocket computer, which he took home without first checking for classified information. While subsequent investigations by his facility failed to find any classified information in the transferred files, Applicant's actions were deliberate and express security violations. His actions are isolated, though, and successfully mitigated by demonstrated overall judgment and reliability in handling classified systems and information. Clearance is granted.

CASENO: 04-04264.h1

DATE: 01/12/2006

DATE: January 12, 2006

In re:

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

Applicant for Security Clearance

ISCR Case No. 04-04264

DECISION OF ADMINISTRATIVE JUDGE

ROGER C. WESLEY

APPEARANCES

FOR GOVERNMENT

Jennifer I. Campbell, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant, with an otherwise unblemished record of protecting and safeguarding classified information, committed a deliberate security violation by downloading unclassified files from his facility's classified computer onto his pocket computer, which he took home without first checking for classified information. While subsequent investigations by his facility failed to find any classified information in the transferred files, Applicant's actions were deliberate and express security violations. His actions are isolated, though, and successfully mitigated by demonstrated overall judgment and reliability in handling classified systems and information. Clearance is granted.

STATEMENT OF THE CASE

On August 5, 2005, the Defense Office of Hearings and Appeals (DOHA), pursuant to Executive Order 10865 and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992, issued a Statement of Reasons (SOR) to Applicant, which detailed reasons why DOHA could not make the preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant, and recommended referral to an administrative judge to determine whether clearance should be granted, continued, denied or revoked.

Applicant responded to the SOR on August 31, 2005, and requested a hearing. The case was assigned to me on October 31, 2005. Pursuant to notice of November 3, 2005, a hearing was scheduled for November 15, 2005, for the purpose of considering whether it would be clearly consistent with the national interest to grant, continue, deny or revoke Applicant's security clearance. A hearing was convened as scheduled on November 15, 2005. At hearing, the Government's case consisted of four exhibits; Applicant relied on one witness (himself) and three exhibits. DOHA received the transcript (R.T.) on December 1, 2005.

PROCEDURAL ISSUES

Before the close of the hearing, Department Counsel moved to amend the subparagraph 1.a to conform with applicant's testimony as follows: Applicant was suspended without pay for one week and placed on six months probation, substituting one week for the alleged two weeks. There being no objection, and good cause being shown, Department Counsel's amendment motion was granted. Applicant's answer remained unchanged by the substitution.

SUMMARY OF PLEADINGS

Under Guideline K, Applicant is alleged to have downloaded files from the classified network to his personally owned USB storage device without authorization in March 2003, in violation of paragraph 5-100 of the DoD 5220.22-M of the national Industrial Security Program Operating Manual (NISPOM) of January 1995, in order to expedite work at home after normal duty hours, for which he was suspended without pay for two weeks and placed on six months probation.

For his answer to the SOR, Applicant admitted downloading his files to his personally-owned storage device in March 2003, in order to expedite work at home after normal duty hours, but denied being suspended without pay for two weeks (claiming just one week of suspension without pay). He claimed to have had no subsequent or prior security clearance violations.

STATEMENT OF FACTS

Applicant is a 41-year old senior software engineer for a defense contractor who seeks to retain his security clearance. The allegations covered in the SOR and admitted by Applicant are incorporated herein by reference adopted as relevant and material findings. Additional findings follow.

While working late at his work site in March 2003, Applicant experimented with a memory card transfer procedure on his classified computer to see if he could download unclassified files from his company's classified system to his personally owned USB storage device (or memory card reader) and then check the card through his digital assister

(PDA). He had previously removed unclassified files from his classified computer in accordance with his classification procedures. Having small children at home, this enabled him to work on projects in his residence and avoid longer on-duty hours. But he had never before experimented with removing unclassified files from his classified computer using a memory card reader and wasn't sure he could do it.

To perfect his experiment, Applicant first inserted the memory card into the system administrator's personal computer (PC). Because this PC is controlled so that only the system administrator can log on, he could not log in (*see* exs. 2 and 3; R.T., at 24). So, he then tried logging in on a colleague's PC that was configured for users and, successful, he installed the memory card reader into this classified computer and accessed the device (exs. 2 and 3). From here, Applicant downloaded his unclassified files he created to the memory card reader and verified the file transfer by inserting the memory card into his personal digital assister (PDA), a pocket computer device he obtained outside the facility (R.T., at 24, 41-42). Applicant then removed his memory card reader and PDA, secured the area and left the facility for home with the devices in his possession.

The following morning (March 7, 2003), Applicant deleted his downloaded files from his memory card reader through the use of his PDA before delivering his memory card and PDA to his facility security officer (FSO). Shortly thereafter, the system administrator tried to log onto her office's PC and was told it needed a reboot. When the FSO was notified of the system administrator's log on problems later in the same day, he asked a security representative in his office to request Applicant to immediately retrieve his memory card reader, his PDA and his personal home computer and bring them to the security office for the FSO to examine (exs. 2 and 3).

Several days later (*i.e.,* on March 12, 2003), the FSO and others in the office installed Applicant's memory card reader (identified by the FSO as a "thumb drive") to ascertain what data was on the memory card (R.T., at 51-52, 56). Unable to spot any files Applicant had downloaded from the classified system, the FSO and his system team conducted a forensic evaluation of Applicant's PDA to check for files downloaded by Applicant. The team found all of the data on Appellant's memory card to be unclassified (R.T., at 54) and none of Applicant's downloaded files on his personal PC (*see* ex. 3; R.T., at 56).

By deliberately introducing a personal memory card reader and a PDA into a DoD closed classified network system without consulting security or system administrator personnel, Applicant disregarded in-place security procedures in violation of paragraph 5-100 of the DoD 5220.22-M of the NISPOM. He neither availed himself of approved trusted downloading procedures, designed to prevent inadvertent downloading of classified data, nor checked his PDA for classified information before transmitting the device to his home and back. At the time, he wasn't sure these downloading actions violated security policy (R.T., at 32).

Applicant's records do not reveal any prior security incidents or violations. But because the files were deleted from Applicant's memory card reader through the use of his PDA, the FSO was unable to determine precisely whether any of the removed data on the memory card was classified or not. Applicant's assurances there were no classified data in the unclassified files he created and subsequently downloaded to his memory card reader are corroborated by his FSO (*compare* R.T., at 24-25, 38, 54). While the facility's adverse information report confirmed only that the FSO's review uncovered no DoD classified or proprietary information on the PC hard drives (*see* ex. 3; R.T., at 34), the FSO's further hearing clarification provides sufficient corroboration of Applicant's no-classified assurances to make them fully credible and worthy of acceptance. Inferences warrant, accordingly, that none of the data transferred to Applicant's memory card reader and PDA contained classified information.

Applicant received annual briefings on handling classified information in compliance with the NISCOM (R.T., at 37). His most recent such briefing of his security responsibilities prior to the March 2003 incident in issue was in June 2002. Applicant acknowledged this June 2002 briefing in writing (*see* exs. 3 and C; R.T., at 28-29). The briefing included instructions on approved downloading procedures and the barring of personal computing devices in the facility. Since his suspension was lifted, he has continued to receive annual security briefings (R.T., at 35). Applicant assures that his only purpose in downloading files from his classified network and placing them in his memory card reader and PDA was "to see if the classified computers would recognize and allow access to the memory card device." He had no intention of keeping the unclassified files, only to verify that the procedure would work (*see* ex. 2).

Both the memory card and PDA used by Applicant to download classified files were secured in a company safe located in the company's security office, pending completion of the investigation (*see* ex. 3). The memory card was permanently confiscated, and its contained data was deleted. Applicant's PDA and personal computer have since been returned to Applicant. Due to the circumstances of his deliberate security violation, he was sanctioned by his manager (who cited the nature of the violation and explained the consequences for future violations, up to and including employment dismissal) and subjected to one week of suspension without pay (*see* exs. 3 and 4). In April 2003, Applicant signed the agreement of understanding outlining the nature of the security violation and potential future consequences for any repeated security violations.

Since his March 2003 security incident, Applicant has performed above expectations and has regained much of the trust he enjoyed with his software team before the incident (*see* exs. A and B). He is valued by his contractor team for both his technical and trouble shooting skills. He credits his challenges in regaining his team's trust following his security breach with his demonstrated improvements in both his technical skills and peer mentoring activities.

POLICIES

The Adjudicative Guidelines of the Directive (Change 4) list Guidelines to be considered by judges in the decision making process covering DOHA cases. These Guidelines require the judge to consider all of the "Conditions that could raise a security concern and may be disqualifying" (Disqualifying Conditions), if any, and all of the "Mitigating Conditions," if any, before deciding whether or not a security clearance should be granted, continued or denied. The Guidelines do not require the judge to assess these factors exclusively in arriving at a decision. In addition to the relevant Adjudicative Guidelines, judges must take into account the pertinent considerations for assessing extenuation and mitigation set forth in E.2.2 of the Adjudicative Process of Enclosure 2 of the Directive, which are intended to assist the judges in reaching a fair and impartial common sense decision.

Viewing the issues raised and evidence as a whole, the following adjudication policy factors are pertinent herein:

Security Violations

The Concern: Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Burden of Proof

By virtue of the precepts framed by the Directive, a decision to grant or continue an Applicant's for security clearance may be made only upon a threshold finding that to do so is clearly consistent with the national interest. Because the Directive requires Administrative Judges to make a common sense appraisal of the evidence accumulated in the record, the ultimate determination of an applicant's eligibility for a security clearance depends, in large part, on the relevance and materiality of that evidence. As with all adversary proceedings, the Judge may draw only those inferences which have a reasonable and logical basis from the evidence of record. Conversely, the Judge cannot draw factual inferences that are grounded on speculation or conjecture.

The Government's initial burden is twofold: (1) It must prove any controverted fact[s] alleged in the Statement of Reasons and (2) it must demonstrate that the facts proven have a material bearing to the applicant's eligibility to obtain or maintain a security clearance. The required showing of material bearing, however, does not require the Government to affirmatively demonstrate that the applicant has actually mishandled or abused classified information before it can deny or revoke a security clearance. Rather, consideration must take account of cognizable risks that an applicant may deliberately or inadvertently fail to safeguard classified information.

Once the Government meets its initial burden of proof of establishing admitted or controverted facts, the burden of persuasion shifts to the applicant for the purpose of establishing his or her security worthiness through evidence of refutation, extenuation or mitigation of the Government's case.

CONCLUSION

Appellant comes to these proceedings as an software engineer who violated established procedures in place for downloading classified computer systems in place. Issues pertaining to his March 2003 one-time violation of NISPOM procedures by downloading unclassified computer files from his classified computer and transferring the files to his personal memory card reader and PDA without following approved downloading procedures or checking his PDA for classified information. That no classified information was actually uncovered in the ensuing office investigation does not eliminate the security significance of the procedural violation.

Moreover, although the files Applicant downloaded from his classified PC in March 2003 contained no uncovered classified information, the memory card reader and PDA containing the downloaded files posed a continuing risk of including classified materials. For Applicant made no precautionary check of either storage unit to ascertain whether classified information was included before he downloaded the files. That neither of Applicant's downloading and transmission violations involved knowing mishandling of classified information does not deprive them of security concerns.

Under the Directive's security violation guidelines in force, persons responsible for safeguarding classified information in their custody and control are required to keep the materials secured in designated areas and to avoid actions that might place classified information under their custody and control at risk to compromise. Applicant's deliberate downloading actions, while undertaken for experimental purposes, expressly violated the procedural requirements of paragraph 5-100 of the NISPOM for using network systems selected for storing classified information. His actions warrant one of the disqualifying conditions (DC) of the Adjudicative Guidelines for security violations: DC E2.A11.1.2.2 (*Violations that are deliberate or multiple or due to negligence*).

The importance of safeguarding classified information cannot be overemphasized. Protecting the nation's security interests against the risks of foreign coercion and intimidation remains a core governmental responsibility that finds roots in our earliest Constitutional history and enjoys the sustaining force of the courts. *Cf. United States v. Curtiss-Wright Corp.,* 299 U.S. 304, 319-20 (1936). What is to be weighed in this case are the deliberate actions taken by Applicant in experimenting with his employer's classified computers to test his ability to download unclassified files and place them in a memory card for retransfer to a pocket computer for home transfer and use. Applicant's failures to seek counseling for his intended downloading actions and/or check the classified PC and transfer units for included classified information increased the security risks for potential compromise of classified information.

In appraising the security significance of Applicant's security violations, careful consideration was given to Applicant's full and open disclosure of his actions in the internal review that followed his actions, his lack of any knowledge of classified information in the files he downloaded, his absence of any acknowledged classified information in all but two of the incidents, his otherwise clean record of observing security procedures for protecting classified information, and his positive contributions to his employer's classified software program. This whole person assessment is consistent with the guidance articulated by the Appeal Board for appraising an applicant's trustworthiness in light of isolated security violations. *See* ISCR Case No. 03-04145 (February 10, 2004) and ISCR Case No. 01-03397 (May 20, 2002).

Applicant's explanations of mishandling his classified computer system, memory card reader, and PDA in his possession and control are sufficient to extenuate and mitigate the security violations attributable to him. Based on the isolated nature of his imprudent action in handling classified equipment, Applicant may take advantage of two of the mitigating conditions under the guidelines for security violations: E2.A11.1.2.2 (*Were isolated or infrequent*) and E2.A11.1.2.4 (*Demonstrate a positive attitude towards the discharge of security responsibilities*)

Furthermore, Applicant has exhibited remorse and renewed understanding about the importance of protecting classified information in his custody and control. His avoidance of any other security violations, his contributions to his employer, and his exhibited attitudinal changes are noted. Based on his otherwise good track record for protecting classified information, his expressed remorse, and his avoidance of any recurrent violations in over two years, he can be assured of complying with security procedures and requirements in the future. Applicant carries his evidentiary burden in demonstrating he meets the high standard of eligibility to access classified information. Favorable conclusions warrant with respect to subparagraph 1.a covered by Guideline K.

In reaching my decision, I have considered the evidence as a whole, including each of the E2. 2.2 factors enumerated in the Adjudicative Guidelines of the Directive.

<u>FORMAL FINDINGS</u>

In reviewing the allegations of the SOR and ensuing conclusions reached in the context of the FINDINGS OF FACT, CONCLUSIONS, CONDITIONS, and the factors listed above, this Administrative Judge makes the following FORMAL FINDINGS:

GUIDELINE K (SECURITY VIOLATIONS): FOR APPLICANT

Sub-para. 1.a: FOR APPLICANT

DECISION

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

Roger C. Wesley

Administrative Judge