DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:)
)
---------------------------)
SSN: -------------------) ISCR Case No. 08-04110
)
)
Applicant for Security Clearance)

Appearances

For Government: James F. Duffy, Esquire, Department Counsel
For Applicant: *Pro Se*

November 4, 2009

Decision

MALONE, Matthew E., Administrative Judge:

Based upon a review of the pleadings, the government's exhibits (Gx.), Applicant's exhibits (Ax.), and Applicant's testimony, his request for a security clearance is granted.

On March 8, 2006, Applicant submitted a Security Clearance Application (SF-86) to renew a security clearance required for his job with a defense contractor. After reviewing the results of the ensuing background investigation, adjudicators for the Defense Office of Hearings and Appeals (DOHA) issued Applicant a set of written interrogatories regarding potentially adverse information in his background. Based on the results of the background investigation and his response to the interrogatories, DOHA adjudicators were unable to make a preliminary affirmative finding[1] that it is clearly consistent with the national interest to continue Applicant's clearance. On October 31, 2008, DOHA issued to Applicant a Statement of Reasons (SOR) alleging

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

facts which raise security concerns addressed in the revised Adjudicative Guidelines (AG)[2] under Guideline M (use of information technology systems).

On December 19, 2008, Applicant responded to the SOR and requested a hearing. The case was assigned to me on June 23, 2009. Pursuant to a Notice of Hearing issued on July 6, 2009, I convened a hearing on July 30, 2009, at which the parties appeared as scheduled. The government presented four evidentiary exhibits included in the record without objection as Gx. 1 - 4. The government also proffered four documents for purposes of administrative notice, which were included in the record as judicial exhibits (Jx.) I - IV.[3] Applicant testified and submitted four exhibits admitted without objection as Ax. A - D. Also included in the record are 10 documents attached to Applicant's response to the SOR.[4] DOHA received the transcript of hearing (Tr.) on August 7, 2009.

Findings of Fact

The single allegation (SOR ¶ 1.a) in this case is as follows:

> On or about January 15, 2004, you were investigated for using your government computer to improperly and without authorization, access computer systems at [an American military installation], for having installed on your computer inappropriate and non-sanctioned software, and having downloaded to your assigned computer's hard-drive classified information regarding contracts for which you were not authorized to [sic] access and had no justification for doing so. The investigation revealed that your activities, which lasted from October 2003 and [sic] January 2004, violated base computer policy. As a result of the investigation you were reassigned and barred from computer access on the Base during the remainder of your assignment there.

On June 17, 2009, the government moved to amend the SOR by removing the word "classified." There being no objection at hearing, I granted the government's motion. (Tr. 11) Accordingly, the information at issue was either business-sensitive or other information to which Applicant allegedly was not authorized access.

In response to the SOR, as to the allegation that he was not authorized to access the information systems, or parts thereof, at the military installation where he worked, Applicant denied that he did so without authorization. He claimed that his access was both verbally authorized and inherently part of his assigned duties as a Functional Systems Administrator (FSA). As to the allegation that he downloaded and stored on his

[2] The revised Adjudicative Guidelines were approved by the President on December 29, 2005, and were implemented by the Department of Defense on September 1, 2006. Pending official revision of the Directive, the revised guidelines replace the guidelines contained in Enclosure 2 to the Directive.

[3] Identified in the transcript at pp. 24 - 33.

[4] Identified in the transcript at pp. 14 - 19.

government computer unauthorized software, Applicant admitted doing so. However, he claimed that, while the software was not authorized, he obtained the software in an effort to improve his ability to perform his FSA duties. In response to the allegation that he improperly, and without authorization or need, downloaded to his computer hard-drive contract information, Applicant again denied that he was not authorized access to that information. He also asserted that the information at issue was inadvertently downloaded, and that whatever was downloaded was not released outside of any Department of Defense computer system. In addition to the admissions of fact contained in Applicant's answer, I make the following additional findings of relevant fact.

Applicant is a 39-year-old network systems engineer. He and his wife have been married since April 1994, and they have two children (ages 14 and 11). In August 2005, he began working for a temporary agency that placed him with a defense contractor, which hired him as a full-time employee in November 2005. He still works for that contractor as a senior network administrator and site manager. Applicant enjoys a good reputation for reliability, honesty, and professionalism at his current company. (Answer to the SOR) He is studying for his bachelor's degree in computer management, and has nine more classes to complete. Applicant was in the United States Navy from January 1991 until January 1999. He served as an aviation electronics technician (AT) and was honorably discharged as a second class petty officer (paygrade E-5). (Gx. 1; Tr. 56 - 57, 61 - 62, 106)

In March 2002, Applicant was hired by a defense contractor to work as an FSA at an overseas U.S. military installation. The company's contract with that installation called for base-wide support for information technology systems management and assurance, as well as a host of other facilities support services. The contract was known as the Base Maintenance Contract (BMC) and was valued at $22 million over five years. (Gx. 3)

The base where Applicant worked was divided organizationally into functional departments for Civil Engineering (CE), Communications, Contracts, and Quality Assurance (QA). CE was responsible for all facilities maintenance and construction matters. Communications was responsible for all matters related to IT systems.

Each department had its own computer servers dedicated to storing and processing their information on an IT system, which was used throughout the military branch involved here. It stored and processed information across departments concerning contracts, fuel, supplies, construction, facilities maintenance, and other matters related to running the base. Access to each server was generally limited to personnel within a given department. However, because of their duties, some personnel had access to multiple or all servers across departmental boundaries.

On December 12, 2002, Applicant was appointed as his company's operations supervisor for all IT matters within CE. (Attachment to SOR Answer) He testified that his duties also included assignment as a QA representative for the principle IT system he worked on. For access purposes, Applicant was assigned as a work group manager (WM), which, by system design, allowed him access to a variety of servers, including the Contracts Server. (Tr. 58 - 62)

The Contracts Department handled matters ranging from requisition of supplies to contract bids, contract performance monitoring, contract awards, and other business-related matters for the command. Contained in the Contracts Server was, in relevant part, information about contracts between the military facility and its defense contractors, including the BMC itself. Other information ranged from the actual contract and bid specifications to Powerpoint slides presenting information about costs and other measures of contractor performance. (Gx. 3)

On January 15, 2004, military investigators were advised that there had been several instances of unauthorized access into the Contracts Server by an employee of Applicant's company. The investigation quickly yielded information sufficient for agents to seize Applicant's government computer. On January 16, 2004, Applicant's access to government IT systems was cancelled and he was assigned other duties pending completion of the investigation. Specifically, it was found that over a three-month period ending on January 8, 2004, Applicant accessed the Contracts Server up to 30 times. It was also found that Applicant accessed the government computer assigned to a military officer in the Contracts Department at least 20 times. During the three-month period in question, Applicant was on holiday leave for 19 days between December 2003 and January 2004. (Gx. 3; Attachments to Answer)

Inspection of Applicant's government computer showed that a copy of the BMC was located on the hard drive. Applicant explained that he did not intentionally "download" the BMC. While testing the vulnerabilities of the base-wide IT system, he accessed the Contracts server as a WM. The BMC file was created using one application, but he opened the BMC file in an application different from the one the file was created in. When exiting the file, he was prompted to decide whether to save the file in the application he used rather than the original application. He asserted that he said "yes," but that the result was that a copy was saved to his computer. (Tr. 97) He did not explain why he answered "yes" rather than leave the BMC in its original state, or why he did not delete it from his computer, or why there were other related files on his computer. He also did not explain why he had to access the Contracts Server more than 30 times, or the officer's computer more than 20 times, or the BMC itself to test system vulnerabilities.

Inspection of Applicant's computer also showed that he had stored several software applications on his computer. Applicant acknowledged that he needed permission from the designated point of contact (a junior enlisted person at either the E-3 or E-4 paygrade) in the base Communications Department before downloading or installing any hardware on his computer. He claimed he did so as to some of the software, but also admitted there were several unauthorized software applications stored on his computer. He knew at the time that only software on an approved list could be loaded onto DoD computers. However, he also claimed that he did not actually install any of the software. He looked at it to see if he could use it in support of his FSA duties. He had intended to transfer the software to a compact disk, but he did not explain why he would even keep the software. (Answer to SOR; Gx. 3; Tr. 53 - 56, 68 - 76)

Investigative interviews were conducted with personnel and technicians, both military and civilian, from the Contracts and Communications Departments. Several of those interviewed questioned whether anyone outside of the Contracts Department should have access to the contracts server. (Gx. 3) However, the same investigative report also showed that the Applicant had broad access throughout the system by virtue of his designation as a WM. The IT system was set up so that all WM's had access across the system regardless of whether they worked in CE or QA or Contracts.

The investigative report also found that Applicant had complained to the Communications Department about this configuration and suggested that it be changed to be more restrictive as to who had access to various data bases, including the Contracts Server. Three times the permissions were changed, but each time the permissions were reinstated. Applicant explained that this occurred because of the way the system was designed. Once that was changed, the restricted access remained permanent. (Gx. 3, Section 2-3; Tr. 88 - 92)

The investigation into Applicant's actions did not result in any disciplinary action against the Applicant. The report of investigation did not contain any conclusions about what happened or about culpability. Further, there is no indication that the information Applicant accessed was ever compromised or used for improper purpose. The report did not cite any specific regulation or procedure at the base or from other authority that Applicant may have violated. Finally, there was no finding that any of the software was actually installed in the DoD system in question, or that the software was designed or intended for malicious purpose.

In January 2004, Applicant lost his access to the information systems and was assigned other duties pending the outcome of the investigation. In July 2004, he took extended leave due to a death in the family. When that leave expired, he asked for and was granted a two-year leave of absence, because he did not want to sit idle pending completion of the military's investigation into his conduct. He was never advised of any investigative conclusions. His employment with that contractor ended in August 2006 when he let pass the deadline for advising the company that he was returning from his leave of absence. (Ax. A)

Department Counsel asked that administrative notice be taken of four documents or publications. All four provide guidance and definitions regarding DoD information systems management and protection. Department Counsel specifically cited section 4.19 of DoD Directive 8500.1 (Jx. I), which requires that software available from public sources "shall only be used in DoD information systems to meet compelling requirements." DoD Instruction 8500.2 (Jx. II) provides extensive definitions within the DoD Information Assurance Program and provides guidance for implementing that program. However, neither party argued for application of any specific provision of that document to the facts in this case. Jx. III is the instruction that provides network user licensing and network professional certification guidance for the military branch Applicant was supporting. It addressed the FSA by saying that FSA's "must thoroughly understand the customer's mission and stay completely knowledgeable of the hardware and software capabilities and limitations." (Jx. III, p. 12) Of WM's, this document stated, "WMs possess developed knowledge of hardware, software, and communications principles, and install, configure, and operate client/server devices. They resolve day-to-day administrative and technical problems users experience and contact their . . . FSA or [help desk] if they cannot resolve their problem." (Jx. III, p. 13) Finally, Department Counsel cited in Jx. IV, an excerpt from the Federal Acquisition Regulations System (FARS), which generally prohibits unauthorized disclosure of "contractor bid or proposal information or source selection information before the award of a Federal agency procurement contract to which the information relates." (48 C.F.R. § 3.104-4(a))

Policies

Each security clearance decision must be a fair, impartial, and commonsense determination based on examination of all available relevant and material information,[5] and consideration of the pertinent criteria and adjudication policy in the Revised Adjudicative Guidelines (AG). Decisions must also reflect consideration of the factors listed in ¶ 2(a) of the new guidelines. Commonly referred to as the "whole person" concept, those factors are:

> (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.

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. In this case, the pleadings and the information presented by the parties require consideration of the security concerns and adjudicative factors addressed under AG ¶ 39 (Guideline M - Use of Information Technology Systems).

A security clearance decision is intended to resolve whether it is clearly consistent with the national interest[6] 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 then falls to the applicant to refute, extenuate or mitigate the government's case.

[5] Directive. 6.3.

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

Because no one has a "right" to a security clearance, an applicant bears a heavy burden of persuasion.[7]

A person who has access to classified information enters into a fiduciary relationship with the government based on trust and confidence. Thus, the government has a compelling interest in ensuring each applicant possesses the requisite judgment, reliability and trustworthiness of one who will protect the national interests 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 in favor of the government.[8]

Analysis

Use of Information Technology Systems

The government allegation in SOR ¶ 1.a, if proved, would raise a security concern addressed in AG ¶ 39 as follows:

> 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.

I have considered the available disqualifying factors listed under AG ¶ 40 as these facts apply to them. At the outset, the facts and circumstances of this case do not require or support consideration of the disqualifying conditions listed at AG ¶ 40(b) (*illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system*), AG ¶ 40(c) (*use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system*), AG ¶ 40(d) (*downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system*), AG ¶ 40(g) (*negligence or lax security habits in handling information technology that persist despite counseling by management*), and AG ¶ 40(h) (*any misuse of information technology, whether deliberate or negligent, that results in damage to the national security*).

As to AG ¶ 40(a) (*illegal or unauthorized entry into any information technology system or component thereof*), and AG ¶ 40(e) (*unauthorized use of a government or other information technology system*), it does not appear that Applicant's access to the

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

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

Contracts Server or the officer's computer was either illegal or unauthorized. Within the broad terms of his job description as an FSA and his access as a WM, along with the access designed into the IT system in question, it appears it was perfectly legitimate for Applicant to access both components. It may be that the IT system should not have been designed to allow him access as he was a contractor employee. But all of the available information shows that he was authorized to access the files and information in question. The more salient question is whether it was acceptable for a contractor to access the BMC or other such information. At the very least, his actions created the appearance of impropriety, in that, as a contractor, he possessed information that potentially could have given his company an unfair advantage when it came to bidding on renewal of the contract in question. However, there is no information about whether the contract was due for renewal, or whether the information was passed to anyone who might use it for that purpose.

Unanswered by the Applicant are reasonable questions regarding the number of times he accessed the Contracts Server and the officer's server in such a brief period. He claimed he was required to test the IT system vulnerabilities, and to maintain and improve the system's efficiency. He has not explained why he accessed the Contracts Server or the officer's computer so many times, or, for that matter, why it was necessary to access those particular aspects of the IT system in the first place. However, because Applicant denied the aspect of this allegation regarding access to the IT system, the government was required to present sufficient reliable information to show that his access was "illegal or unauthorized," and not simply improper or unwise. AG ¶ 40(a) does not apply.

The disqualifying condition at AG ¶ 40(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*) must also be considered. It is uncontroverted that Applicant stored software on his government computer he knew was not on a list of approved software. However, it was not established that the software that was actually installed and was in use on his computer. Nonetheless, his actions constituted "introduction" for purposes of AG ¶ 40(f), and Applicant knew it was prohibited to put the software on his computer as he did. AG ¶ 40(f) applies.

By contrast, the record as a whole also supports the mitigating condition at AG ¶ 41(a) (*so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur or does not cast doubt on the individual's reliability, trustworthiness, or good judgment*). It has been more than five years since Applicant left his position pending the outcome of the investigation. There is, as yet, no conclusion by those involved with the investigation about whether Applicant did anything to justify revocation of his system access. Since leaving that job, he has worked for his current employer with good results and without incident. His referrals praise his reliability and expertise, and it does not appear that he has or will repeat his past mistakes regarding software introduction. The other mitigating conditions under AG ¶ 41 do not apply.

As to any specific rules, procedures, guidelines, or regulations that may have been violated, the information presented through Jx. I - IV provided definitions helpful in understanding Applicant's FSA and WM duties. At the DoD level, Jx. I made clear that software introduction should be done pursuant to a "compelling requirement." However, there is nothing in the record, especially in the Report of Investigation (ROI) in Gx. 2, that cites specific rules or procedures, either instituted by the base military organization or by Applicant's company, that he violated. Further, other than the opinions of those interviewed during the investigation, the ROI contains no conclusions about procedural or rules violations, and no conclusions about culpability. On balance, I conclude the security concerns raised by the available information are mitigated.

Whole Person Concept

I have evaluated the facts presented and have applied the appropriate adjudicative factors under Guideline M. I have also reviewed the record before me in the context of the whole person factors listed in AG ¶ 2(a). Applicant is 39 years old, married for more than 15 years, and the father of two. He is also a veteran of the U.S. Navy and has been steadily employed without incident since his honorable discharge in 1999. He is also studying for a bachelor's degree related to his field of expertise. Aside from an inconclusive investigation into his access to an IT system for which he was, at least partially responsible, there is no information that would support a conclusion that Applicant's judgment, reliability, and trustworthiness are not sufficient for purposes of access to classified information. A fair and commonsense evaluation of this record shows that the security concerns raised by Applicant's conduct relative to information technology systems are mitigated. Any doubts about Applicant's suitability for access to classified information have been satisfied.

Formal Findings

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

Paragraph 1, Guideline M:	FOR APPLICANT
Subparagraph 1.a:	For Applicant

Conclusion

In light of all of the foregoing, it is clearly consistent with the national interest to grant Applicant's request for access to classified information. Request for security clearance is granted.

MATTHEW E. MALONE
Administrative Judge