DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 12-10692
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Alison O'Connell, Esq., Department Counsel

For Applicant: Alan V. Edmunds, Esq.

10/20/2014

_____

Decision

_____

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

Based on a review of the pleadings, exhibits, and testimony, I conclude that Applicant has not mitigated the security concerns raised under the guideline for use of information technology systems. His request for a security clearance is denied.

Statement of the Case

On March 27, 2014, the Department of Defense (DOD) issued to Applicant a Statement of Reasons (SOR) that detailed security concerns under Guideline M (use of information technology systems). This action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry (February 20, 1960),* as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program (January 2, 1992)* as amended; and the Adjudicative Guidelines (AG) implemented by the Department of Defense on September 1, 2006.

In his Answer to the SOR, Applicant admitted both allegations under Guideline M. The Defense Office of Hearings and Appeals (DOHA) issued a Notice of Hearing on July 28, 2014, setting the hearing by video teleconference on August 19, 2014. At the hearing, I admitted into evidence seven Government exhibits (GE 1-7). I marked the Government's exhibit list as Hearing Exhibit (HE) I, and the Government's discovery cover letter as HE II. Applicant testified, offered the testimony of one additional witness,

and offered eight exhibits, admitted into evidence as AE A-H. DOHA received the transcript of the hearing (Tr.) on August 28, 2014.

Findings of Fact

Applicant's admissions are incorporated as findings of fact. After a thorough review of the pleadings and the evidence, I make the following additional findings of fact.

Applicant is 38 years old. He earned a bachelor's degree in 1998, and expects to complete a master's degree in information security and assurance in 2015. He married in 2009 and has two children, who are two and four years old. He has worked in information technology (IT) for more than 10 years, and has held the position of senior systems administrator for several defense contractors. He was granted his first security clearance in 2001. Applicant worked for Company A, a defense contractor, from 2010 to 2012. He began working for his current employer in November 2012. (GE 1; AE D-F; Tr. 53-54)

While employed by Company A, Applicant and his two team mates supported two government agencies, Agency B and Agency C. Company A was contracted to Agency B. Company A also provided IT support to Agency C. Agency B was located at a different site from Applicant's, and did not provide support to his location; but it allowed him to handle computer problems that arose in his location. Agency B provided Applicant with an administrator user name and password so that he could log on as an administrator when necessary to solve IT issues. (GE 2, 6; AE A, C; Tr. 27-51)

In about February 2012, Applicant and his team members were having problems printing. Applicant found that if he logged on using administrator privileges, he was able to print. He elevated his rights to administrator level, installed the printer, and it became available for Applicant and his team mates' use. He testified that he intended to remove the administrator privileges and return to his user-level account, but forgot to do so. He also testified that it "[i]s unsustainable to log off and log back on all day long to make this function happen, to print." He continued to use his account with the administrator privileges. When questioned at the hearing why he did not immediately remove the administrator privileges after installing the printer, he testified, "I do not recall the circumstances as to why I did not." (GE 2; AE A; Tr. 57, 67-72)

During an April 2012 interview with representatives of Agency B and his employer, Applicant was asked if he had "browsed the web while logged onto his [work computer] under your administrative account." Applicant replied that he did browse the web to research work-related issues, program downloads, troubleshoot, and research college-related course information. He also admitted that he surfed the web while the administrator privileges were still on his account, and did not remove the administrator privileges after solving the printer problem. He said he did not intentionally leave the

privileges on his account. He admitted that he did not need to have the administrator privileges while surfing. (GE 3) Agency B investigators noted in their incident report that,

> Surfing the web as an administrator exposes the [Agency B] network to an unacceptable level of risk. The reason being that if a machine is compromised by a user having administrative privileges, the malicious software would be able to propagate unencumbered throughout a network because it would assume the privilege level of the compromised user. (GE 6 at 3)

Applicant's Company A supervisor testified that he did not agree with this assessment because the computers were not connected to a government network. Applicant agreed, noting in his written explanation of events that his laptop was not on the (Agency B] network and therefore, any programs on his laptop would not affect the [Agency B] network. (GE 3, 6; AE A, C; Tr. 44-45) However, the Agency B disagreed, stating in its incident report,

> Users who have been entrusted with privilege of being administrators function with two accounts. Normal duties are performed as a normal user, and administrative tasks are performed with the elevated administrator account. In this instance [Applicant] destroyed that separation by utilizing his administrator account to elevate his personal user account with administrative rights. Thus presenting the [Agency B] network with an unacceptable level of risk. (GE 6)

On March 13, 2012, Applicant was at work using his government laptop. He was taking an online college course, which was approved by his division director. The training related to coursework for "ethical hacker" certification. A virus alert appeared on his screen. He received a call from the computer security office, advising him to run a virus scan, provide the results, and disconnect from the Internet. Applicant ran the scan, which completed on the following morning, March 14. It showed no viruses on his laptop.[1] He forwarded the results to the computer security office. The following day, March 15, Applicant was told to complete a questionnaire regarding the incident. His computer was forwarded to Agency B. He also was required to leave the facility until cleared to return.[2] (GE 2, 3, 5; AE A, B)

[1] Investigation by government security personnel initially showed that hacking tools, including password-cracking software, resided on Applicant's work computer. Applicant denied any knowledge of how this software appeared on his system. He also testified that nothing other than the alert was found, *i.e.*, no file, and that sometimes virus alerts are "false positives" that occur when no virus or malware is present. Applicant's supervisor testified that, to his knowledge, no evidence was discovered to show hacking programs resided on Applicant's work computer. The SOR alleges that Applicant installed unauthorized software on his government computer, but it does not allege that he installed hacking tools or malicious software on it. (GE 3; Tr. 32-33, 76)

[2] Applicant's access to classified information was suspended on an interim basis on May 3, 2012. His security clearance remained suspended as of the date of the hearing. (GE 7; Tr. 54)

During March and April 2012, Applicant completed two additional questionnaires. Also in April, Applicant met with representatives of Agency B and Company A. Following the forensic analysis performed on his computer, he was asked about two particular software programs that were discovered on his work laptop's hard drive (Programs 1 and 2). Applicant was informed that one of the programs was a password-cracking tool (Program 1). He denied any knowledge that this software, or any other hacking tools, resided on his laptop. During his security interview with a DOD investigator in August 2012, Applicant again denied downloading or installing any such tools.[3] (GE 2, 3, 5; AE A)

At the hearing, Applicant testified that Program 2 was a business tool that he installed on his government laptop in order to test it. During his April 13 interview, he said he downloaded it to his work laptop "[w]ith the intention of researching the viability and potential for it on our internal network." He also stated, "I did not have specific authorization to download [Program 2] to this laptop." During Applicant's August 2012 security interview, he discussed a telephone conference with representatives of Agency B, who asked if he had downloaded software without authorization. He stated he told the representatives that he had not. In his Answer to the SOR, Applicant admitted downloading software without authorization. (Answer; GE 2, 3; AE A)

In his Answer to the SOR, Applicant stated he was confused about who to ask for authorization: "I lost sight that these were supposed to be managed by [Agency B] (because our site managed them), therefore I needed their permission to install any software." However, at the hearing, when asked if he knew he should have sought authorization, he testified it was not until after the fact that he knew he had to obtain authorization. (Answer; Tr. 64-65) Applicant testified he thought he had latitude to download software because his job was to

> [p]rovide solutions, to issues and problems. And I didn't believe that I every [*sic*] if I asked [Agency C] or [Agency B] every time to try to fix a problem, I probably wouldn't get any work done, honestly. So that was, that's my rationale. (Tr. 64)

The program manager who supervised Applicant from 2010 to 2012 testified. He has held a top secret security clearance since 2001, and was a senior network engineer in the 2010-2012 time period. He testified that in March 2012, Agency B was investigating attempted hacking into its IT systems. He stated, "[a] remote detection system had identified Applicant's computer as having several types of viruses or programs that could be used for malicious intent, specifically hacking or password gathering." Ultimately, a hacker was not discovered, and his understanding is that no evidence was found to show that any virus or hacking programs resided on Applicant's

---

[3] DOHA provided Applicant with a copy of the summary of his August 7, 2012 security interview with an authorized DOD investigator. He was asked to review the contents and correct any inaccuracies. He made no changes, and adopted the summary as accurately reflecting his interview. (GE 2)

work computer. He stated that the software Applicant downloaded was Program 2, a commonly used business program, not a hacking tool. He opined it was possible that Agency C might have supported downloading Program 2, but Agency B might not have been aware it was downloaded. He testified, "It is my belief that there is no, there was no unauthorized software on these workstations from an [Agency C] perspective." (Tr. 27-51)

During cross-examination, the witness stated that the team was "[g]iven great latitude to download software tools and research them for business purposes" but they were first required to obtain approval:

> MS. O'CONNELL: And were all those tools you had to receive approval before you could download those software tools?
>
> [WITNESS]: I would say yes. Yes. (Tr. 42)

As to the issue of administrator privileges, the witness said Agency B gave the team members a username and password to log in as an administrator when necessary. However, Agency B did not give them authorization to change their own personal user accounts to administrator-level accounts. (Tr. 45-48)

Applicant's character reference from his current employer noted his reliability and positive feedback from the client. His 2010 through 2012 performance evaluations noted his expertise in information assurance, his striving for mastery of his field, and his professionalism. In 2010 and 2011, he was rated either "excellent" or "meets standards" in all categories. Applicant received a 2011 Certificate of Appreciation from Agency C. His friend, a lay minister, noted Applicant's honesty. Other friends noted his integrity, and described him as trustworthy, sincere, and hardworking. (AE D, G, H)

Policies

Each security clearance decision must be a fair and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the AG.[4] Decisions must also reflect consideration of the factors listed in ¶ 2(a) of the Guidelines, commonly referred to as the "whole-person" concept. The presence or absence of a disqualifying or mitigating condition does not determine a conclusion for or against an applicant. However, specific applicable guidelines are followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified information. In this case, the pleadings and the information presented by the parties require consideration of the security concerns and adjudicative factors addressed under Guideline M (use of information technology systems).

[4] Directive. 6.3.

A security clearance decision is intended only to resolve the question of whether it is clearly consistent with the national interest[5] 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. Because no one has a "right" to a security clearance, an applicant bears a heavy burden of persuasion.[6] A person who has access to classified information enters into a fiduciary relationship with the Government based on trust and confidence. Therefore, 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 her or his 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.[7]

Analysis

Guideline M, Use of Information Technology Systems

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

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

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

> (e) unauthorized use of a government or other information technology system; and

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

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

[7] *See Egan;* AG ¶ 2(b).

(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.

In his Answer, Applicant admits SOR allegation ¶1.a, that he installed software on his government computer system without authorization. The software was Program 2, a business tool. Although Applicant's supervisor testified that the team was given leeway to download and research software tools for business purposes**,** he also stated that the team members were required to seek authorization to download such software. The initial suspicion that Applicant also downloaded a hacker tool, Program 1, was not substantiated, and is not alleged in the SOR. AG ¶ 40(f) applies to his installing Program 2 on his government computer. Applicant also admitted to SOR allegation ¶1.b, that he added administrator privileges to his personal IT user account without authorization, and surfed the web using an administrator-level account. AG ¶ 40(e) applies.

AG ¶ 41 provides the following relevant mitigating conditions:

(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available; and,

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

The events at issue occurred more than two years ago, which is not recent. However, they did not occur under unusual circumstances that are unlikely to recur, but rather in the normal course of Applicant's work, in the field in which he continues to be employed. His actions raise doubt about his reliability and judgment. AG ¶ 41(a) applies in part.

Applicant receives some mitigation under AG ¶ 41(b) regarding the downloading of Program 2, because he downloaded it to research whether it would improve the agency's efficiency. However, his actions in upgrading his account to administrator level, leaving it at that level instead of returning to his personal account, and then surfing with an administrator's privileges, were not minor. Agency B determined that Applicant's surfing the web under an account with administrator privileges resulted in

an unacceptable level of risk. Applicant receives only partial mitigation under AG ¶ 41(b).

As to AG ¶ 41(c), I cannot confidently conclude that Applicant's actions were unintentional, because of the conflicting information he provided about his knowledge of the requirement to seek authorization to download software. In his Answer, he admitted he downloaded software without authorization, but "lost sight of" the fact that he should do so. Also, when questioned by Agency B on April 20, 2012, he admitted he downloaded software without authorization. However, his testimony at the hearing conflicted with these statements, when he testified he did not know he had to seek authorization, and only learned it later, through the investigation process. In addition, there is no evidence that he notified his supervisors about the downloading at any point before the Agency B investigation began. AG ¶ 41(c) does not apply.

Whole-Person Analysis

Under the whole-person concept, an administrative judge must evaluate the applicant's security eligibility by considering the totality of an applicant's conduct and all the circumstances. An administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

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

Applicant is a mature adult, and a responsible husband and father. He has worked in IT for more than 10 years, providing support to DOD contractors. His friends laud his dependability and honesty. He has received solid performance evaluations and praise from his supervisor, who testified at his hearing. Moreover, Agency B's investigation did not find that Applicant downloaded or installed any malicious software or hacker's tools.

The fact that Applicant sought out software, Program 2, to maximize the efficiency of his agency's IT systems is not at issue. However, Applicant's disregard for

the requirement to obtain authorization to download and install Program 2 on a government computer is a concern. His supervisor testified that the team members were required to obtain such authorization. Also of concern is Applicant's attitude toward the requirements. As to the need for authorization, he testified that he "wouldn't get any work done" if he had to seek authorization every time. Regarding the requirement to return to his regular user-level account after upgrading to administrator level to fix IT issues such as the printer, he testified that it was "unsustainable" to repeat that action whenever he needed to fix a problem. Applicant's willingness to place his own desire for convenience above the Government's requirements is a security concern.

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

Formal Findings

Paragraph 1, Guideline M	AGAINST APPLICANT
Subparagraphs 1.a – 1.b	Against Applicant

Conclusion

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

RITA C. O'BRIEN
Administrative Judge