DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 14-00153
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Stephanie C. Hess, Esq., Department Counsel
For Applicant: *Pro se*

12/22/2014

_____

Decision

_____

COACHER, Robert E., Administrative Judge:

Applicant failed to mitigate the security concerns under Guideline M, use of information technology systems; and Guideline E, personal conduct. Applicant's eligibility for a security clearance is denied.

Statement of the Case

On March 13, 2014, the Department of Defense Consolidated Adjudication Facility (DOD CAF) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline M, use of information technology systems; and Guideline E, personal conduct. DOD CAF acted under Executive Order (EO) 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).

On May 22, 2014, Applicant answered the SOR and elected to have his case decided on the written record. Department Counsel submitted the Government's File of Relevant Material (FORM) on September 30, 2014. The FORM was mailed to Applicant who received it on October 14, 2014. Applicant was given an opportunity to file objections and submit material in refutation, extenuation, or mitigation. He did not submit any further information. The case was assigned to me on December 5, 2014.

Findings of Fact

In Applicant's answer to the SOR, he denied all the Guideline M allegations, but failed to either admit or deny the Guideline E allegations. However, since the Guideline M allegations are all cross-alleged under Guideline E, I will take his nonresponse to these allegations as denials. After a thorough and careful review of the pleadings and evidence, I make the following findings of fact.

Applicant is 30 years old. He is single and has no children. He currently works as a security engineer. He began working for his current employer in August 2013. He holds a master's degree. He has no military service and has never held a security clearance.[1]

Applicant's conduct raised in the SOR includes: (1) gaining unauthorized access to webpages, servers, and personal information of random persons stored on personal and corporate information systems between February and April 2013 (SOR ¶ 1.a); (2) uploading and deleting files from privately-owned webservers without proper authorization between February and April 2013 (SOR ¶ 1.b); (3) uploading programs onto information technology systems (ITS) without authorization, which allowed him browser and root access to servers between February and March 2013 (SOR ¶ 1.c); (4) using default credentials without authorization to sign into privately-owned network printers between February and April 2013 (SOR ¶ 1.d).

Applicant's security clearance application was certified in September 2013. He responded affirmatively to a question concerning his use of ITS, which specifically asked if he had illegally or without proper authorization accessed or attempted to access any ITS within the last seven years. When asked to describe the nature of the incident, Applicant wrote the following concerning his actions in February 2013:

> With cleverly crafted google queries, I was able to find documents that people had uploaded to the internet that contained information including their usernames and passwords for websites or servers. I attempted to log in to these systems to look around. There are, I would estimate, about 1,000 incidents of this nature, If I could successfully log in to whichever system the credentials belonged to, I did one of three things: 1. In the majority of cases I looked around the file system of various log files to see what its owner was using it for. If another unauthorized user had obviously

[1] Item 4.

> been modifying the system, I deleted malicious files, killed their processes, and occasionally blocked the IP of someone if they were obviously intruding. In a few cases, I contacted the owners to alert them to the security risk. 2. If the system was a web server, I uploaded a modified version of the b374k shell to have browser access to the server. 3. If I had root access, I created a new root user to have later access to the server.[2]

He described a second incident involving unauthorized access in February 2013 by stating, "Some network printers have public IP addresses and a web interface, so google finds them. I used default credentials to sign into some printers to see what capabilities and settings they had."[3]

He was also asked in the application if, in the last seven years, he illegally or without authorization modified destroyed, manipulated, or denied others access to information residing on an ITS, or attempted to do so. He responded affirmatively and described his actions in February 2013 as follows:

> As indicated in the section on unauthorized accesses, I gained access to machines because people posted their usernames/passwords online. I deleted files on machines if the files were plainly unwanted by the machine's owners.[4]

He further responded affirmatively when asked if, in the last seven years, he introduced, removed, or used hardware, software, or media in connection with any ITS without authorization. He explained his affirmative response by stating, "As stated previously, I removed malicious software from machines that I did not have permission to access."[5]

In Applicant's answer, he offers explanations for the way he completed his security clearance application. He stated that although he did not have written or verbal authorization to access the accounts, he believed permission to access them was implied because of the availability of the public servers. He also stated that he took these actions as an "academic research activity" and that he followed all the "responsible disclosure" rules, which are known in the computer security community. He did not provide written documentation of these rules or any other documents that would corroborate his position.[6]

---

[2] Item 4.

[3] Item 4.

[4] Item 4.

[5] Item 3.

[6] Item 4.

Applicant's specific responses to the SOR allegations are as follows: SOR ¶ 1.a: He admitted he did not have written permission to access the system, but he had login credentials that were publicly available and linked from Google; SOR ¶ 1.b: He admitted to uploading one file to multiple webservers. This file allowed him access to the server. He deleted files if there was documentation indicating that they were malicious; SOR ¶ 1.c: He denied uploading or installing any programs on the systems that he accessed. He stated that he only used programs that were previously installed on the systems to gain access; SOR ¶ 1.d: He stated that the printers he accessed were publicly available. He concludes his answer by stating the following:

> All of these instances took place over a short period of time, while I was in school. I was academically interested in the structure of real-world computers and networks. I realized quickly that this was an inappropriate way to gain the skills that I was interested in, and I stopped completely. My behavior does not show a pattern over a wider time frame, either before or after. [7]

Policies

When evaluating an applicant's suitability for a 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 used 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 overarching 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, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or

[7] Item 3.

mitigate facts admitted by applicant or proven by Department Counsel, and 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 an 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 M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern pertaining to 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 reliably 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 conditions that could raise a security concern and may be disqualifying. I considered the following relevant:

> (a) illegal or unauthorized entry into any information technology system or component thereof; and
>
> (b) illegal or unauthorized modifications, destruction, manipulation, or denial of access to information, software, firmware, or hardware in an information technology system.

Applicant accessed numerous (his estimate was 1,000) ITS without authorization, including private or sensitive information. He also uploaded an

unauthorized program (b375k) and deleted files without authorization. Both AG ¶ 40(a) and AG ¶ 40(b) apply.

I have considered all of the mitigating conditions under AG ¶ 41 and considered the following relevant:

> (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.

Applicant's conduct was intentional, recent, and occurred on numerous occasions. Although he claims to have acted in furtherance of his academic curiosity, he also admitted that he quickly realized that what he was doing was wrong. His actions show a degree of unreliability, untrustworthiness, and bad judgment. Additionally, insufficient time has passed to determine whether he has truly learned from these incidents and modified his behavior. AG ¶ 41(a) does not apply.

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern for personal conduct:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying in this case. The following disqualifying condition is relevant:

> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group.

Applicant's action in accessing personal computer files without authorization, demonstrates untrustworthy and unreliable behavior. He knew his actions were wrong, yet he gained such unauthorized access about 1,000 times. AG ¶¶ 16(d) and 16(e) apply.

The guideline also includes conditions that could mitigate security concerns arising from personal conduct. I have considered all of the mitigating conditions under AG ¶ 17 and especially considered the following:

> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and
>
> (d) the individual has acknowledged the behavior and obtained counseling to change or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

Applicant's conduct in gaining unauthorized access to unknown persons' computer files 1,000 times is not minor. It casts doubt on his reliability, trustworthiness, and good judgment. AG ¶ 17(c) does not apply. He acknowledged his wrongdoing, but he provided no evidence that he has taken positive steps to alleviate the factors that caused his actions, nor provided sufficient evidence establishing that such behavior will not recur. AG ¶ 17(d) partially applies.

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 the applicant's conduct and all the circumstances. The 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.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I considered Applicant's youth and explanation for why he engaged in the concerning behavior. However, Applicant's blatant disregard for the privacy of others when he accessed their computer files without

authorization raises a significant security concern involving his trustworthiness and lack of good judgment.

Overall, the record evidence leaves me with questions and doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant did not mitigate the security concerns arising under Guideline M, use of information technology, and Guideline E, personal conduct.

Formal Findings

Formal findings for or against Applicant 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:	AGAINST APPLICANT
Subparagraphs 1.a - 1.d:	Against Applicant
Paragraph 2, Guideline E	AGAINST APPLICANT
Subparagraph 2.a:	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 Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Robert E. Coacher
Administrative Judge