KEYWORD: Information Technology

DIGEST: Applicant is 41 years olds and has been employed as an information systems security manager by a defense contractor since August 2005. While working at a federal agency, he was accused of inappropriately doing tasks on information systems that he was unauthorized to do. He has mitigated the use of information technology systems security concerns. Clearance is granted.

CASENO: 06-08839.h1

DATE: 05/31/2007

DATE: May 31, 2007

In re:	)	
	)	
----------	)	ISCR Case No. 06-08839
SSN:----------	)	
	)	
Applicant for Security Clearance	)	

DECISION OF ADMINISTRATIVE JUDGE
JACQUELINE T. WILLIAMS

APPEARANCES

FOR GOVERNMENT
Richard A. Stevens, Esq., Department Counsel

FOR APPLICANT
Jerome H. Gress, Esq.

SYNOPSIS

Applicant is 41 years olds and has been employed as an information systems security manager by a defense contractor since August 2005. While working at a federal agency, he was

accused of inappropriately doing tasks on information systems that he was unauthorized to do. He has mitigated the use of information technology systems security concerns. Clearance is granted.

STATEMENT OF THE CASE

On August 16, 2005, Applicant executed an Electronic Questionnaire for Investigations Processing (e-QIP).[1] On December 29, 2006, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR)[2] to Applicant, detailing the basis for its decision–security concerns raised under Guideline M (Use of Information Technology Systems) of the revised Adjudicative Guidelines (AG) issued on December 29, 2005, and implemented by the Department of Defense for SORs issued after September 1, 2006. The revised AG were provided to Applicant when the SOR was issued.

In a document, dated January 23, 2007, Applicant responded to the SOR allegations and requested an in-person hearing. The case was assigned to me on February 22, 2007. A Notice of Hearing was issued on February 28, 2007, scheduling the hearing for March 14, 2007. The hearing was rescheduled because Applicant retained counsel. Another Notice of Hearing was issued on March 16, 2007, scheduling the hearing for April 3, 2007. A Notice of Appearance was filed by Applicant's attorney on March 21, 2007. The hearing took place as scheduled. At the hearing, the Government offered five exhibits, Exs. 1-5, and Applicant offered one exhibit, Ex. A. All exhibits were admitted into the record without objection. The transcript (Tr.) was received on April 16, 2007.

FINDINGS OF FACT

Applicant denied the allegations under Guideline M, subparagraphs 1.a through 1.f. After a complete and thorough review of the evidence in the record, and upon due consideration of same, I make the following findings of fact:

Applicant is 41 years olds and has been employed as an information systems security manager by a defense contractor since August 2005.[3] He has a bachelor's of science degree in business. In 1992, he received a master's of science degree in information systems.[4] He also teaches courses on information security at a local university. His teachings include a lecture on ethics, styled after his professional experiences in that area.[5] He was married in October 1998 and has three children.

---

[1]Ex. 1 (Electronic Questionnaire for Investigations Processing, dated August 16, 2005).

[2]Pursuant to Exec. Or. 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended (Directive).

[3]Tr. 16.

[4]Tr. 19.

[5]Tr. 16-17.

From 1993 to October 1997, Applicant worked at a government agency as the systems administrator, managing the email system.[6] A few months after he started working, he was accused of improperly accessing a coworker's email on at least one occasion without her permission or knowledge. He admitted accessing a female coworker's email because she asked him to reset her password, providing him access to her email inbox.[7] He looked in the email inbox because he had asked her out on a date and wanted to see her response. He only looked at the email that she had sent to him.[8] While there, he received three exceptional ratings or awards.[9]

In 1997, Applicant was promoted to a senior engineer at the same agency. He was accused of improperly accessing his team leader's computer and email on at least one occasion without his permission or knowledge. Applicant admitted that this incident occurred but:

> . . . it was with his [team leader's] knowledge. It wasn't necessarily without his knowledge. He routinely asked, when he was traveling, he would routinely ask for us to – to access his computer to check his emails.[10]

Applicant testified that he was able to access his team leader's email "[b]ecause he gave me the user ID and password. He gave it to all 15 of us on his team."[11] He revealed that his team leader had threatened him in the past, specifically, when Applicant told his superior that it was inappropriate to execute a particular task.[12] Applicant filed a grievance indicating the task he was asked to do was inappropriate. Holding a copy of Applicant's grievance, his team leader stated "[y]our life at [agency] is over."[13] He repeated it twice. Applicant was scared. He was motivated to look at the email because "I wanted to see if I was in any harm." Classified information was not accessed.[14]

In 1997, he was accused of improperly copying at least one "ZIP file" from his team leader's computer without his permission or knowledge. Applicant testified that he had no recollection of this activity and denied doing it.[15]

---

[6]Tr. 20-21.

[7]Tr. 20-21.

[8]Tr. 22.

[9]Tr. 20.

[10]Tr. 23.

[11]Tr. 24.

[12]Tr. 25.

[13]Tr. 26.

[14]Tr. 26.

[15]Tr. 27.

While continuing to work at the same federal agency, Applicant was charged with improperly performing computer attacks, outside the scope of his employment and authority, against the agency's computer systems. Applicant indicated that he did this task with authorization from his team leader.[16] The purpose was to go into the email system and identify trivial or easy passwords created by users. After that, Applicant:

> . . . called them [user] on the phone and said, 'you need to change your password in the system.' Because it's my [Applicant's] responsibility to manage the contractors that are supporting that system, I requested that those contractors reset the passwords, or ordered that they have the password be changed for those users.[17]

Applicant averred that his team leader was next to him when he executed the computer attacks.[18] These computer attacks occurred approximately three to six times between 1996 and 1997. Applicants' employment at the agency was terminated in October 1997.[19]

On February 12, 1999, Applicant was denied SCI access by NSA. On May 4, 1999, following his appeal, NSA's denial of his SCI access was sustained.[20]

Applicant had three character witnesses testify on his behalf at the hearing. The first witness currently is an information systems security specialist at a federal agency and has a top secret security clearance with special accesses.[21] She first met Applicant in 1997 at the federal agency where they both worked. They worked together for two and one-half years, but they have managed to stay in touch.[22] She recalled that several colleagues had direct access to the team leader's email password and user identification, a direct violation of security protocol.[23] She was aware that Applicant had the team leader's user identification and password but she never saw Applicant access his email.[24] The team leader had asked her "if we had enough money on my contract with [contractor] to hire some infoware specialists."[25] "Infoware specialists are people who try to do penetration testing and things of that nature to try to break in [internal computer system]."[26] Upon hearing her negative response, the team leader stated "well, I guess we'll just have to do it in-

---

[16]Tr. 28.

[17]Tr. 31.

[18]Tr. 29.

[19]Tr. 30.

[20]Ex. 5 (First Appeal Review, dated May 4, 1999).

[21]Tr. 66-67, 70.

[22]Tr. 67.

[23]Tr. 69, 72-73.

[24]Tr. 74.

[25]Tr. 74-75.

[26]Tr. 75.

house."[27] She testified that after this conversation, Applicant was called into the team leader's office, and the computer attacks began shortly thereafter. She indicated that Applicant was very smart, with the highest integrity, but naive, in that "he never questioned management."[28]

The second witness was employed as a senior security consultant and met Applicant on the job in either 1997 or 1998.[29] He and Applicant "worked on many jobs together, and traveled all around the world together."[30] He and Applicant continued to work together at different job locations, have kept in touch, and socialize outside of work.[31] He implicitly trusts Applicant, and Applicant has the keys to his house.[32] Also, "[h]e [Applicant] has access to my systems, and I don't give that out readily. I – in fact, he's the only one that has access to any of my systems."[33] Applicant told him about the computer attacks and he testified that "[h]e [Applicant] thought that his boss had authority to do that."[34] As a self-employed consultant, he is paid to do computer attacks for his customers.[35] He acknowledged that when he worked with Applicant, he was "very well respected, a phenomenal technical person. Very good with the clients."[36]

The third witness was Applicant's supervisor for a little more than two years. The week after the hearing, the witness was to be director of strategic capture for another defense contractor.[37] He has known Applicant for at least four years. When he met him, he was impressed with Applicant's credentials.[38] He requested that Applicant seek a security clearance.[39] He knew about the email and computer attacks. He stated:

> It's not unusual for someone in the position [Applicant] was in, especially at his age, but in a position he was in, to be asked to do what he did. It is not unusual. I

---

[27]Tr. 75.

[28]Tr. 75.

[29]Tr. 90, 91.

[30]Tr. 91.

[31]Tr. 92.

[32]Tr. 92.

[33]Tr. 92.

[34]Tr. 94.

[35]Tr. 95.

[36]Tr. 96.

[37]Tr. 100-101.

[38]Tr. 102, 107-108.

[39]Tr. 103.

have done it. I have asked subordinates to crack accounts . . . . And so I've asked that to be done because we needed that information.[40]

In a letter dated April 2, 2007, another character reference stated he has worked for the federal government in the intelligence and security fields for more than 15 years.[41] During the past year, he has personally witnessed Applicant's integrity when working with him on several highly sensitive and critical initiatives for the government. "In all of my dealings with [Applicant], I have found him to be an honest and trustworthy person, who consistently follows agency rules and guidelines."

POLICIES

"[N]o one has a 'right' to a security clearance."[42] As Commander in Chief, the President has "the authority to . . . control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position . . . that will give that person access to such information."[43] The President authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so."[44] An applicant has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his or her security clearance. The clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials.[45] Any reasonable doubt about whether an applicant should be allowed access to sensitive information must be resolved in favor of protecting such sensitive information.[46] The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of an applicant. It is merely an indication that the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.[47]

The revised Adjudicative Guidelines set forth potentially disqualifying conditions (DC) and mitigating conditions (MC) under each guideline. Additionally, each security clearance decision must be a fair and impartial commonsense decision based on the relevant and material facts and circumstances, the whole-person concept, along with the adjudicative process factors listed in listed in the Directive and AG ¶ 2(a).

---

[40]Tr. 113 -114.

[41]Ex. A (Character witness letter, dated April 2, 2007).

[42]*Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

[43]*Id.* at 527.

[44]Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960).

[45]ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002).

[46]*Id.*; Directive, ¶ E2.2.2.

[47]Exec. Or. 10865 § 7.

Conditions that could raise a security concern and may be disqualifying, as well as those which would mitigate security concerns, together with the whole-person, are set forth and discussed in the conclusions section below.

CONCLUSIONS

I have carefully considered all the facts in evidence and the legal standards, and I reach the following conclusions.

Misuse of information technology systems, under Guideline M, is always a security concern because the 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. The Government has established a *prima facie* case for disqualification under Guideline M, use of information technology systems.

Applicant testified that after a female colleague asked him to change her email password, he read an email message that she had sent him. He did this because he had asked her out on a date and was curious about her response. He did abuse his position as an administrator of the agency's system. His behavior at that time was inappropriate and created a violation of trust that he had. Moreover, after being threatened by his team leader, he went into his email mailbox to read a message to see if or how he was going to be harmed. Thus, Use of Information Technology Systems Disqualifying Condition (IT DC) ¶ 40(a) (*illegal or unauthorized entry into any information technology systems or component thereof*) and IT DC ¶ 40(b) (*illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system*) apply.

Various factors can mitigate misuse of information technology systems concerns. Applicant is a smart, respected individual, trusted by the colleagues who testified about his character. He was also presented as naive and doing what was asked, rather than inquiring about the legalities or authority concerning what he was told to do. He credibly testified about accessing his team leader's email, but he insisted that it was done at the bequest of the supervisor. The second witness corroborated his testimony and indicated that she knew that several people were given access to the team leader's user identification and password, which she believed was against security protocol. Applicant's testimony was convincing when he spoke about the computer attacks he performed, authorized by his team leader. His testimony was corroborated by the first witness who was asked by the team leader if funds were available to get a contractor to do the job. When he was informed that there was no money for a computer attack, he told her it would be done by in-house staff, and he gave that responsibility to Applicant. The second witness testified that he is paid to do computer attacks for his customers. Based on all of the testimony, I conclude that if Applicant was attacking his federal agency's computer system without authorization, he would have been stopped after the first attack. Moreover, he would not have had an opportunity to successfully complete additional attacks on the same computer system. All of the witnesses gave him accolades for his professionalism, honesty, and trustworthiness. Thus, Use of Information Technology Systems Mitigating Condition ¶ 41(a) (*so much time has passed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not case doubt on the*

individual's reliability, trustworthiness, or good judgment) applies. Applicant has mitigated the Government's case. Accordingly, allegations 1.a through 1.f of the SOR are concluded in favor of Applicant.

I have considered all the evidence in the case. I have also considered the "whole person" concept in evaluating Applicant's risk and vulnerability in protecting our national interests. I am mindful that he was denied SCI access in 1999 and lost his appeal of that decision. His immaturity and low self-esteem, allowed him to snoop into emails that he was unauthorized to access for his own personal perusal. I conclude that those negative traits are behind him and occurred more than 10 years ago. Applicant has matured, and is a well-respected worker. He is a more polished, knowledgeable, and savvy employee. Applicant is by all accounts a hard-working man, although naive at times, and he has forged relationships with coworkers over the years. They took the time to testify on his behalf, and have not wavered in their trust of him With the acquisition of more professional experience, he has honed his business acumen and now knows how to act, interact, and react to directives given to him by those in superior positions. He has developed a presence that allows him to inquire, if necessary, about the appropriateness of tasks that he has to execute. Because he is smart, and highly thought of at work, he is more assured about his skills and voice in the workplace because his colleagues believe in him as a responsible member of the team. There is no reason for Applicant to deviate from displaying the appropriate professionalism in any work environment in the future. For the reasons stated, I conclude Applicant is suitable for access to classified information.

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 (Use of Information Technology Systems): FOR APPLICANT

Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	For Applicant
Subparagraph 1.c:	For Applicant
Subparagraph 1.d:	For Applicant
Subparagraph 1.e:	For Applicant
Subparagraph 1.f:	For Applicant

DECISION

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

Jacqueline T. Williams
Administrative Judge