DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-14118
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Alison O'Connell, Esq., Department Counsel
For Applicant: Diane Schuster, Personal Representative

09/20/2013

Decision

MARSHALL, Jr., Arthur E., Administrative Judge:

Applicant mitigated the Government's security concerns under the guideline for misuse of technology information system. His eligibility for a security clearance is granted.

Statement of the Case

On June 4, 2013, the Department of Defense (DOD) sent Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline M (Misuse of Technology Information Systems). The action was taken under Executive Order 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) effective within the DOD on September 1, 2006.

In a June 14, 2013, response to the SOR, Applicant denied the sole allegation raised and requested a hearing before an administrative judge. The case was assigned to me on July 25, 2013. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on July 26, 2013, setting the hearing for August 13, 2013. The hearing

was convened as scheduled. The Government offered Exhibits (Exs) 1-4. Applicant objected to two of the documents, arguing that the documents contained hearsay. The Government correctly noted that hearsay is admissible in an administrative proceeding. The Government also noted the reliability of the documents due to their creation in the regular course of business. I accepted the documents with assurances they would be reviewed and afforded appropriate weight after examination. (Transcript (Tr.) at 15-18) Applicant gave testimony, introduced three witnesses, and offered one document, which was accepted into the record as Ex. A without objection. The transcript was received on August 21, 2013. Also on August 21, 2013, the Government forwarded one additional document from the Applicant, which was accepted without objection as Ex. B. The record was then closed.

Findings of Fact

Applicant is a 39-year-old senior enterprise management architect. He has worked for his present employer for approximately three-and-a-half years. Applicant has earned a bachelor's degree in business administration with a concentration in information technology. He is single and has no children.

From about 2000 to 2010, Applicant worked in the area of information technology for a company. The information technology department consisted of Applicant, who was the head of the division, and one other individual, the Tier 1 Support Engineer. (Tr. 99) For many years Applicant reported to the president. At some point prior to mid-January 2010, there was a restructuring that led him to report to a vice president of the company. (Tr. 45) Until at least November 2009, Applicant regularly provided administrative password information and updates to this vice president. (Tr. 48)

Applicant was terminated from his position as Director of Information Technology on January 22, 2010. The basis for his dismissal was a poor managerial decision he made based on inaccurate data he had been provided. (Tr. 42-43) Applicant believed this was an excuse owing to an increasing difference in business viewpoints. (Tr. 81) As is customary, he was escorted out of the building that afternoon. The only information solicited by his employer for transitional purposes were the passwords to the systems, which he previously had provided multiple times and in multiple formats (Tr. 27, 48) Applicant believed this request of information to help the company transition to his eventual successor was deficient. (Tr. 27) In retrospect, as their former information technology director, he finds their lack of protection glaringly deficient.

Applicant further notes that the company failed to follow its usual protocols in changing his passwords and other access terms or devices upon his departure. (Tr. 82) There was no attempt to block his access to the company's computer and Internet system. There is no evidence that upon his departure or soon thereafter, that a replacement or temporary replacement was in position within the information technology office to actively preclude Applicant from accessing its systems.

That weekend, Applicant left for a previously planned vacation abroad. He enjoyed the weeklong vacation, then returned home on Monday, February 1, 2010. (Tr. 37). Applicant received several calls from three former colleagues, two senior consulting engineers and the Tier 1 Support Engineer who worked under Applicant before Applicant's dismissal. (Tr. 62, 64, 75, 88-89) With Applicant dismissed, the Tier 1 Support Engineer comprised the entire information technology division. (Tr. 99) The three former colleagues requested help from Applicant for gaining access to their company's systems. Apparently, some passwords were not working. He assumed they were soliciting help with company passwords in order to further the company's business. He knew their work necessitated access through various passports and firewalls. (Tr. 54-57, 88-89) These employees were accustomed to going to Applicant for such help and continued to do so despite his termination. (Tr. 40)

Feeling his one month severance package constructively retained his loyalty, if not his services, for one-month post-termination, he offered answers to their questions. (Tr. 33, 40) He felt that their solicitation of help from him authorized him to provide assistance. (Tr. 61-62, 88-90) He credibly stated, "I believe(d) the moment a representative from (the company) contacted me for aid they were authorizing me to help them." (Tr. 74) Calls regarding the passwords continued despite his initial attempt to help.

On the morning of Tuesday, February 2, 2010, Applicant wondered whether the company had changed administrator passwords after his departure, an appropriate measure the company would regularly have taken. To test the system and see if the passwords had changed, he remotely accessed the business' computer system on his personal laptop from home, using a variety of passwords and by-passing safeguards in a virtual computer application to which he had access while working for the company. (Tr. 90) He was not explicitly asked to do so by the engineers or IT professionals, but he thought it might reveal a problem. (Tr. 61-62) He did not access any information while he was in the system. (Tr. 67, 69) All he did was "authenticate that (he was) logged in. And then (he) shut it back off." (Tr. 66-67)

In accessing the system, Applicant found that it was working as before his termination. (Tr. 70-72). This suggested to Applicant that the company had neglected to implement "an adequate transition plan in order to make sure (his) response, (his) role was covered and (his) responsibilities were addressed by the internal staff there." (Tr. 89) Regardless, the engineers continued to have difficulty using the passwords. (Tr. 60-61) He saw no reason to tell these individuals that he had double checked the system from home. He now laments this failure. (Tr. 61, 67) Accessing the system required considerably more than simply applying passwords. (Tr. 65-66) Still curious as to what the problem was, he accessed the system a second time to see if he could identify their problem. (Tr. 70-72) With no problems to note with the system itself, he opined that the engineers and his former Tier 1 Support Engineer lacked the technological competency to "understand the architecture of the system." (Tr. 64; *see also* Tr. 88-89)

On Thursday, February 4, 2010, the Vice President of Service Delivery messaged Applicant via a social media computer service. This particular vice president was the "number two" officer at the company. (Tr. 78) This was a different vice president from the executive to whom he formerly reported. This vice president wrote: "This is a confidential matter, but you really need to call me as soon as possible," followed by the executive's first name and a telephone number. (Ex. A at 1)

Applicant promptly called his former employer's Vice President, as requested. They discussed the password situation. Applicant gave his former superior pertinent passwords and other access credential information. (Tr. 78) Later that day, the Vice President sent another message: "Evidently, we tried that (password) with no luck. Tried again just a few minutes ago. If you can think of ANYTHING, please let me know." (emphasis in the original, Ex. A at 2)

Before Applicant saw the Vice President's second missive, he received a February 4, 2010, letter by expedited delivery from a law firm. (Ex. 4) It was delivered on, at the earliest, Friday, February 5, 2010, possibly as late as Saturday, February 6, 2010. (Tr. 97) The letter instructed Applicant to direct any communications toward his former employer to the attorney who wrote the letter:

> It has come to our client's attention that you have attempted to access (the company's) computer systems remotely and without authorization on more than one occasion. Moreover, you have additionally manipulated, destroyed, or stolen files contained on those systems without permission. Your actions are illegal and you must cease and desist from such conduct immediately. (Ex. 4)

The letter continued by noting, "(s)pecifically, (the company) has evidence that on several occasions, including as recently as February 3, 2010, you gained or attempted to gain access to (the company's) secure computer systems (remotely)." (Ex. 4) The letter never clarifies whether Applicant was successful in gaining access or whether it only had evidence of an attempt to access their system. If the company did obtain the evidence it alleged, it would suggest that at least one or more of the passwords he provided was correct. (Tr. 63-64)

The letter states that the company "has evidence that (Applicant) deleted at least one file from a server desktop and caused other damage to (the company's) computer systems." (Ex. 4) Attached to the letter is a printout showing Applicant's laptop had successfully accessed the company's system on Tuesday, February 2, 2010, at 8:29 a.m., which is consistent with his testimony. No other evidence was demonstrated. The alleged "manipulated, destroyed, or stolen files" were not identified. (See, *e.g.*, Tr. 93-94)

Eventually, Applicant met with the business' legal representative. The situation was discussed. An allegedly lost or deleted file was never identified, nor was there any evidence showing or suggesting Applicant had "touched, damaged, or altered any kind

of any file." (Tr. 86-87) Then defamation of Applicant's character was discussed. (Tr.85) Ultimately, the matters were dropped. (Tr. 85)

The Executive Vice President and partner of the company during Applicant's tenure stated that he found Applicant to be thorough, highly skilled, and ethical. (Tr. 104-105) He has no concerns regarding Applicant's ability to protect classified material. (Tr. 105) A former colleague at the company serving as a senior consultant described Applicant as having an excellent work ethic, noting, "(Applicant) would constantly go past what was required of him to contribute back to (the company). Even when he was heavily involved in projects, he still would make time to contribute back to the organization he worked for." (Ex. B) The former service delivery manager at the company up to 2009 takes credit for the company finding and hiring Applicant. He finds Applicant to be highly ethical and dependable, noting that he would trust him with classified information. (Tr. 110-112) He does not believe Applicant harbors any animosity toward the company. (Tr. 112) He has a "very hard time believing" the allegations against Applicant. (Tr. 112-113) The Chief Technology Officer during Applicant's tenure at the company stated that he spoke with Applicant directly about the facts at issue. Like Applicant, he has moved on to new work. He fully believes Applicant's explanation -- that the allegations must be based on a misunderstanding since there is no evidence that the company's system was actually damaged. (Tr. 119-120)

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 derived from 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 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 the applicant may deliberately or inadvertently fail to safeguard 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 have considered the following as potentially relevant:

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

> (c) use of any information technology to gain unauthorized access to another system or to a compartmented area within the same system;
>
> (e) unauthorized use of a government or other information technology system; and
>
> (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.

After being dismissed, Applicant accessed his former employer's information system on two occasions. He did so without explicit managerial authorization to do so. Consequently, I find that AG ¶¶ 40(a) and (c) apply with regard to his accessing the company's information system.

Applicant's former employer alleged in vague terms that Applicant had maliciously removed, damaged, or otherwise manipulated the company's information system. Applicant denies this allegation. He credibly testified that he simply accessed the information system, then exited it, in order to see if the passwords worked or if any alterations had been made that would be impeding his former colleagues' access to the system. He similarly testified that when he met with the company's counsel, the only evidence provided by his former company suggesting wrongdoing was his remote access of the company's information system on one occasion. Vague allusions to other wrongdoing were undefined and unsubstantiated. The company dropped the matter once Applicant asserted that their allegations could constitute defamation. Lacking evidence from investigators or the company rebutting Applicant's argument, I find that the Applicant did not act in bad faith when he accessed the company's information system. I further note the absence of evidence showing he did more than enter the system without explicit authorization. I find none of the above disqualifying conditions apply to allegations asserting Applicant performed malignant actions while in the company's system.

I also have considered all of the mitigating conditions under AG ¶ 41. I considered AG ¶ 41(a) relevant:

> 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 actions to help his former colleagues occurred in February 2010, over three-and-a-half years ago. Since that time he has been gainfully employed in a similar capacity and working with similarly protected systems. He maintains a reputation among former colleagues as being highly ethical, loyal, and skilled. The cease and desist letter

regarding his accessing his former company's information system is the only evidence suggesting inappropriate behavior during Applicant's career. However, it is notable that Applicant only got involved with his former colleagues because it was apparent his former assistant was not prepared to handle the transition after Applicant's termination, and because he believed his one-month, post-termination salary payments obligated him to assist the company to some degree during that period.

Applicant's demonstration of loyalty to his former employer is consistent with assessments made by his former colleagues. He now understands that he could have insulated himself from criticism or attack had he first sought and received managerial authorization to help his former colleagues. However, it is understandable how he might have felt he was authorized to access the system if it furthered his attempts to address unsolicited requests for help from his former assistant, senior staff, and later, a vice president. Regardless, since then, he has continued to impress colleagues with his reliability, ethics, and talent; he handles his responsibilities professionally and without incident. There is nothing to suggest that Applicant intentionally sought to harm the company's information system, or that his version of the facts is incorrect. In light of these considerations, I find it unlikely that a similar scenario will ever recur and again raise security concerns. AG ¶ 41(a) 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 relevant circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a). 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 have incorporated my comments under the three above-referenced guidelines in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed above, but some warrant additional comment.

Applicant is a 39-year-old senior enterprise management architect who has worked for his present employer for about three-and-a-half years. He has earned a bachelor's degree and is single. The incidents giving rise to the allegations occurred in early 2010, nearly a decade after Applicant first started working for the former employer. By the time, Applicant was in his late 30s and he had established a reputation for loyalty, ethics, and skill.

Shortly after being terminated from his job as director of information technology in January 2010, Applicant was solicited by three former colleagues, including his former support engineer, who apparently had been left alone in the information technology division after Applicant's dismissal. They needed to check their passwords because the passwords they had were not working. When Applicant's initial aid did not

help, he accessed and immediately withdrew from his former company's information system remotely in order to help his former colleagues. Any concerns he may have had regarding helping these people without explicit authorization seemed allayed when his assistance was solicited by a company vice president.

Although a letter from the company's counsel waged unspecified allegations against Applicant concerning the theft, removal, or other mischief related to the system, it only provided evidence showing that Applicant had once accessed its system after his termination. Applicant credibly testified that when he met with the company's representative, no evidence of wrongdoing was provided or described. Rather, the company's representative apparently backed off when Applicant mentioned the potential for a defamation suit against the company. To date, nothing more has come from the company's allegation.

Since that time, Applicant has continued in his chosen career without further incident. Applicant now understands what he believed to be helping former colleagues was technically an unauthorized entry into his former employer's information system. For this mistake, Applicant is thoroughly contrite. There is no documentary evidence showing he purposefully or negligently damaged the information system, nor that he removed any files. While his entry into the system may have been initially unauthorized, he did not do it maliciously. He did it out of a sense of loyalty, to the company and his former colleagues. There is no direct evidence of actual harm. I am confident that he will not again attempt to access secure systems without explicit authorization. For all these reasons, I conclude Applicant mitigated the security concern arising under the use of information technologies systems guideline (Guideline M). Clearance is granted.

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:	FOR APPLICANT
Subparagraph 1.a:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant a security clearance. Eligibility for access to classified information is granted.

_____

Arthur E. Marshall, Jr.
Administrative Judge