DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-14644
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Philip J. Katauskas, Esq., Department Counsel
For Applicant: *Pro se*

08/16/2013

_____

Decision

_____

CREAN, Thomas M., Administrative Judge:

Based on a review of the pleadings, exhibits, and testimony, eligibility for access to classified information is granted.

Statement of the Case

On July 29, 2011, Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) to obtain a security clearance required for a position with a defense contractor. After an investigation conducted by the Office of Personnel Management (OPM), the Department of Defense (DOD) issued Applicant interrogatories to clarify or augment potentially disqualifying information. After reviewing the results of the background investigation and Applicant's response to the interrogatories, DOD could not make the affirmative findings required to issue a security clearance. On March 29, 2013, DOD issued a Statement of Reasons (SOR) to Applicant detailing security concerns for use of information technology systems under Guideline M and personal conduct under Guideline E. These actions were 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 in the DOD on September 1, 2006. Applicant acknowledged receipt of the SOR on April 3, 2013.

Applicant answered the SOR on May 16, 2012. He admitted in part and denied in part the use of information technology systems allegation under SOR 1.a, and admitted the allegation under SOR 1.b. The same conduct was cross-alleged as personal conduct security concerns under Guideline E. Applicant admitted in part and denied in part the allegation under Guideline E, consistent with his admissions and denials to SOR paragraph 1. He requested a hearing before an administrative judge. Department Counsel was prepared to proceed on June 17, 2013. The case was assigned to me on June 21, 2013. The Defense Office of Hearings and Appeals (DOHA) issued a Notice of Hearing on June 27, 2013, for a hearing on July 30, 2013. I convened the hearing as scheduled. The Government offered two exhibits, which I marked and admitted into the record without objection as Government exhibits (Gov. Ex.) 1 and 2. Applicant testified and offered four exhibits which I marked and admitted into the record without objection as Applicant Exhibits (App. Ex.) A through D. DOHA received the transcript of the hearing (Tr.) on August 7, 2013.

Findings of Fact

After a thorough review of the pleadings, transcript, and exhibits, I make the following essential findings of fact. His admissions are included in my findings of fact.

Applicant is a 38-year-old telecom systems administrator for a defense contractor. He married in 2004 and has no children. He was homeschooled until college. He has two years of college but did not earn a degree. (Tr. 11-12; Gov. Ex. 1, e-QIP, dated July 29, 2011)

The SOR alleges security concerns for both use of information technology systems and personal conduct. Under use of information technology systems, it is alleged that Applicant, between January 2008 and May 2011, intentionally accessed and misused the unlocked computers of coworkers in violation of company policy (SOR 1.a); and between April 2010 and May 2011 he intentionally misused his elevated administrator rights to read text messages and emails of coworkers in violation of company rules and policies (SOR 1.b).

Applicant self-reported these allegations when he completed his security clearance application in July 2011. (Gov. Ex. 1, e-QIP, dated July 29, 2011, section 27) The workstations for Applicant and his co-workers in the information technology department (IT) of their employer were visible to all in the workplace. The company policy was for employees to secure, or lock, their work computer before leaving the workstation unattended. (Tr. 15-36)

The company policy also extended to the actions to take when finding an unlocked computer. The individual finding an unlocked computer was to lock the

computer and notify the co-worker that the computer was left unlocked and should be locked when not attended. However, it was common practice in the IT department to access the unlocked computer, use it, and place some type of funny message or open a funny web browser so the individual knew their computer was left unlocked.

On his security clearance application, Applicant stated that on a number of occasions, he accessed an unlocked coworker's computer, and against company policy left something to indicate it had been left unlocked. His usual practice was to open a funny web page. On one occasion, he sent a message to another IT person in a nearby cubicle who was talking to the person that left their computer unlocked. Both the other workers would know that the computer was left unlocked. After Applicant reported the IT department practices in 2011, the correction procedures were clarified. Now when a computer is discovered unlocked, the members of the IT department lock the computer and place a small sign on the computer to show it had been left unlocked. (Tr. 36-42)

As the telecom administrator for his company, Applicant had enhanced access to the telephone and e-mail system of the company. One of his functions was to monitor the systems to determine that company employees used the systems in accordance with company policy. He monitored the level of phone calls and text messages, as well as whether the use was for business or personal reasons. However, Applicant exceeded his authority by continuing to look at text messages and e-mails beyond that required to perform his job requirements. He continued to look at the information because he was curious. Applicant stopped exceeding his authority in 2011. He self-reported on the security clearance application that on a number of occasions he continued to monitor the systems after making the findings required for his administrator duties. He stopped his action over two years ago when he completed his security clearance application. (Tr. 42-51)

Applicant presented letters of recommendation and accomplishment from co-workers, friends, and family members. A friend wrote that she has known Applicant for over 14 years and observed that he conducts himself ethically and legally in all aspects of his life. He is dedicated to the community and his job. Applicant explained to her the full extent of his wrongful actions as noted above and she understands his violations of company policy. She still finds that he is responsible and trustworthy. She recommends he be granted access to classified information. (App. Ex. A, Letter, undated)

A friend wrote that she has known Applicant for over 13 years. In her opinion, he is sincere, honest, and a professional dedicated to his job. He is responsible and diligent in his work. Applicant informed her of his actions causing security concerns. He told her he was wrong in what he did and it would never happen again. She believes he is sincere. He is an outstanding member of the community. She recommends he be granted eligibility for access to classified information. (App. Ex. B, Letter, undated)

A third friend wrote that she has known Application for over ten years when they worked together at another job and company. Applicant was an eager and hard worker. She never saw him engage in an improper action, or violate rules and regulations. She

finds him to be dependable, reliable, law abiding, and trustworthy, and he exercises good judgment. (App. Ex. C, Letter, undated)

Applicant's brother, an Air Force intelligence officer, wrote that he has known Applicant all of his life. He has seen Applicant's attention to detail and efforts to correctly complete all projects. He discussed the allegations with Applicant. Applicant realizes that he violated the trust placed in him as an IT administrator. Applicant voluntarily stopped his actions when he realized that they were contrary to policy and beyond the scope of his function. He voluntarily reported them on his security clearance application. This indicates that Applicant wants to be completely honest, open, reliable, and trustworthy in his duties. He believes Applicant is trustworthy and capable of protecting classified information. He recommends that Applicant be granted eligibility for access to classified information. (App. Ex. D, Letter, undated)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which must be considered 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. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the Applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The Applicant has the ultimate burden of persuasion for obtaining 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 protect or protect classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information.

Analysis

Use of Information Technology Systems

A security concern is raised by noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems reflecting on an individual's reliability and trustworthiness, and calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include related computer hardware, software, firmware, and data used for the communications, transmission, processing, manipulation, storage, or protection of information. (AG ¶ 39)

Applicant admits he accessed co-workers unlocked computers in violation of company policy to let them know that their computer was left unlocked when it was not being used. Applicant's use of the computer was in violation of company policy which was to not access the unlocked computer but lock the computer and notify the individual the computer was left unlocked. Applicant also admits that he accessed co-workers e-mails, text messages, and other systems beyond what he need to perform his function as the telecom systems administrator. Applicant's actions raise disqualifying condition 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).

Applicant raised the mitigating conditions 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 and does not cast doubt on the individual's reliability, trustworthiness, or good judgment); AG ¶ 41(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 AG ¶ 41(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). These mitigating conditions apply.

Applicant and his fellow IT co-workers used an inappropriate method to alert coworkers they left their computer unlocked when not at their desk. When a computer was left unlocked, the company policy was to lock the computer and notify the individual. Rather than lock the computer, Applicant and his IT co-workers would access or use the unlocked computer to send a message using a funny website or message

that the computer was left unlocked. The process used by the IT workers was unusual and not in compliance with company policy. It was used within the IT department for many years. Applicant self-reported the process that was in violation of company policy and the practice was changed over two years ago to be in compliance with company policy. While Applicant's actions were inappropriate, they were done in the best interest of the organization and in an attempt to have all workers comply with company policy. It was not done with malice or vindictiveness. I find for Applicant as to the allegations under Guideline M.

Personal Conduct:

A security concern is raised because conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information. Personal conduct is always a security concern because it asks the central question whether the person's past conduct justifies confidence the person can be entrusted to properly safeguard classified information. (AG ¶ 15)

Applicant's actions in accessing unlocked computers of his co-workers and exceeding his systems administrator's functions raise the following personal conduct disqualifying conditions:

> AG ¶ 16(c) (credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information);
>
> AG ¶ 16(d) (credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicting that the person may not properly safeguard protected information. This includes but is not limited to consideration of: (3) a pattern of dishonesty or rule violations); and
>
> AG ¶ 16(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).
>
> I considered the following personal conduct mitigating conditions:

> AG ¶ 17(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 is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment);
>
> AG ¶17(d) (the individual has acknowledged the behavior and obtained counseling to change the behavior 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); and
>
> AG ¶ 17(e) (the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress).

As noted above, Applicant's violation of company policy that led to the improper use of the company information technology systems are minor and were not done for wrongful, malicious, or vindictive reasons. Applicant used an improper approach to correct a problem in the IT department. Applicant had the authority to review co-workers phone use, text messages, and e-mail to determine compliance with company policy. He exceeded his authority when he continued to review co-workers accounts after determining the usage was proper and in compliance with company policy. While he exceeded his authority, he acknowledged his errors and stopped the practice. He self-reported his improper actions. I find that the incidents happened under unique circumstances and his improper computer use and the exceeding of his authority are unlikely to recur. Applicant mitigated personal conduct security concerns.

Whole-Person Analysis

Under the whole-person concept, the administrative judge must evaluate an applicant's security eligibility by considering the totality of the 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.

Under AG ¶ 2(c), the ultimate determination of whether to grant 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 that Applicant is highly regarded by his friends and family.

Applicant chose an improper method to correct a problem in the IT department of his employers. He also exceeded at times his authority as the telecom systems administrator. Applicant's actions were wrong but not intended to be harmful or deceitful. They were not reckless, irresponsible, or the result of poor judgment. The actions were minor and unlikely to happen in the future. He realizes his errors and self-reported his actions. His actions and his handling of the incidents do not indicate that he has questionable judgment, is untrustworthy, lacks reliability, or is unwilling to comply with rules and regulations. These incidents do not raise questions about Applicant's reliability, trustworthiness, and ability to protect classified information. The incidents do not indicate Applicant may not properly handle, manage, or safeguard classified information. The record evidence leaves me without questions and doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has mitigated the personal conduct and use of information technology systems security concerns.

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
Subparagraphs 1.a - 1.b:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.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 eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
THOMAS M. CREAN
Administrative Judge