DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 14-03975
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Chris Morin, Esq., Department Counsel
For Applicant: Ronnie Chaney, Personal Representative

12/09/2014

_____

Decision

_____

RICCIARDELLO, Carol G., Administrative Judge:

Applicant mitigated the Government's security concerns under Guideline M, use of information technology systems, and Guideline K, handling protected information. Applicant's eligibility for a security clearance is granted.

Statement of the Case

On September 12, 2014, the Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline M, use of information technology systems, and Guideline K, handling protected information. 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.

On September 25, 2014, Applicant answered the SOR and requested a hearing before an administrative judge. The case was assigned to me on October 28, 2014. The

Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on October 31, 2014. I convened the hearing as scheduled on November 18, 2014. The Government offered exhibits (GE) 1 and 2, which were admitted into evidence without objection. Applicant and two witnesses testified. Applicant offered Applicant Exhibits (AE) A through D, which were admitted into evidence without objection.[1] DOHA received the hearing transcript (Tr.) on November 26, 2014.

Findings of Fact

Applicant denied all of the allegations in the SOR. After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is 49 years old. He served in the Army from 1985 until he honorably retired in paygrade E-8 in 2005. He has been married since 1989, and he has a 24-year-old son and a 30-year-old stepdaughter. He holds two master's degrees. He has held a top secret security clearance with access to sensitive compartmented information continuously since 1985. At different times during his career he has held higher access clearances. He has worked for his current employer since June 2014.[2]

Applicant was employed with Employer A from 2008 to February 2013. As part of his employment he had access to the company's email account. An employee's email account is not monitored while they are employed. Once an employee leaves the company, a supervisor will review the employee's email account to see if there are any questionable issues.[3]

In late January 2013, Applicant submitted his resignation to Employer A, and his last day was in February 2013. Applicant's supervisor, who was the chief executive officer (CEO) of the company, reviewed his email account and contacted the facility security manager because he noticed that Applicant had transferred data from his company account to his personal account. The data included user names and passwords from the company's accounts, the company's accounting practices, and the company's business rating information.[4]

The CEO testified that Applicant had a legitimate reason to have the company's business rating information while he was employed with the company. He would obtain the information from the accounting department. The business rating information is important and sensitive because it evaluates the credit worthiness of the business. Applicant had no need to have this information after he left employment with the

[1] Hearing Exhibit (HE) I is a letter from Applicant's personal representative advising of his intent to appear at the hearing. HE II is Department Counsel's exhibit list. HE III is Department Counsel's letter to Applicant regarding discovery matters.

[2] Tr. Tr. 11, 123, 126, 155-158.

[3] Tr. 31-36.

[4] Tr. 32-36, 50, 56-58.

company. There was also no reason Applicant should have had the user name and password associated with the business rating information while at the company or after he left employment with the company. The CEO confirmed that Ms. W was one of three people who had access to the user name and password on the business rating information account. She worked remotely.[5]

Applicant kept a master list of user names and passwords for all his personal and business accounts. This business and personal list were not separated, but mixed together. The list included user names and passwords for hotels, airlines, and other consumer websites. It also included user names and passwords for the company that would allow access to proprietary information, including the user name and password for the business rating information. Applicant credibly testified that he received this information from Ms. W who had access to the account. Applicant explained that Ms. W sent him the user name and password so he could expedite a proposal that was to go to the CEO, and they wanted to ensure the potential client's finances were sound before the company engaged the potential client. The user name and password were part of the master list. The CEO confirmed that Applicant did not need access to the business rating information for his consultant project. Applicant acknowledged it should not have been transferred. He stated he was not thinking when he transferred the entire list. At the time, he did not think what he was doing was wrong because he intended to come back to the company to work as a consultant.[6]

Applicant had an agreement with Employer A to work as a consultant from February 2013 until June 2013. The agreement was to work on a proposed contract with the government, if the company was awarded the contract. The plan was for the CEO to rehire Applicant, and he would be the program manager. The company would be provided the required documents and aspects of the work after the contract was awarded. There were occasions in the past when contract proposals had been sent to personal email accounts, which was against the rules. Applicant forwarded the proposal for a government contract to his personal email account. The CEO did not believe this proposal pertained to work that was part of the consulting agreement. Applicant explained that it was part of the proposed contract, and he wanted to be ready to start the project once it was awarded. He acknowledged he should have asked the CEO for permission before transferring the document to his personal account.[7]

The accounting information that Applicant forwarded to his personal account provided a blueprint of how the company conducts its business. The CEO testified the document contained proprietary business documents. It was not inappropriate for Applicant to have access to this information while he was employed at the company, but

[5] Tr. 36-39, 70-82.

[6] Tr. 68-69, 96-97, 129-138, 154.

[7] Tr. 39-46, 49, 82-92, 97, 129, 133, 143-145.

it was not a necessary part of Applicant's job. He should not have had access to the information after he left the company.[8]

Applicant explained he had access to the company's accounting information because he wanted to make sure he was in compliance when he worked for the company as a consultant. He explained that while working for the company he needed the information to approve invoices and timesheets. He was concerned that someone might question how he handled the financial matters, so he wanted to make sure he followed the approved practices. Applicant transferred the accounting information to his personal account because he was preparing for the consulting contract that he believed he would be working on. He wanted to be ready to start as soon as the contract was approved. As the program manager, he wanted to make sure the new staff understood what they were required to do. He explained that when the contract was awarded he wanted to be able to staff it right away, and in order to do what he needed to be ready before it was awarded. Applicant acknowledged he should have told the CEO before he sent the material to his personal email account. He admitted he should have asked permission. He credibly testified that he made a mistake and promised to comply with all the requirements in the future.[9]

Applicant's duties at the company included reviewing human resource and accounting policies and procedures. This also included approving timesheets, expense reports, and invoices. He was also responsible for participating in cost proposals, which included salaries, rate buildups and final rates for the contracts.[10]

The CEO confirmed that Applicant was a good worker and there were never any issues regarding his employment. Applicant was never counseled or disciplined for infractions or security-related violations. The CEO thought highly of Applicant and believed he is patriotic. This is what influenced the CEO to give Applicant the consulting contract. The CEO confirmed that it was not authorized or customary for employees to use their home email accounts for work purposes, and it was considered a serious violation. When the CEO discovered the above discrepancies and filed a report, he and Applicant discussed the matter. Applicant agreed to delete all of the data he had transferred from the company account to his personal account. The CEO confirmed that Applicant apologized to him about transferring the data. The CEO is confident that Applicant deleted all of the transferred information. He confirmed that none of the information transferred was compromised or used for Applicant's or another's benefit. He did not believe Applicant intended to harm the company. Despite what transpired, the CEO would recommend Applicant for a position of trust. He believed Applicant's conduct was a one-time transgression.[11]

[8] Tr. 63-67.

[9] Tr. 46-49, 66-67, 138-143.

[10] AE C.

[11] Tr. 51-56, 60-63, 67, 70, 96.

Applicant admitted he made a mistake when he transferred information from his employer's account to his personal email account. He believed he was acting in good-faith at the time. Applicant credibly testified that he purged every document he transferred from the company to his personal account. He never would have made the transfer if he thought he was doing something wrong. He explained that if he had wanted to use the material for an unauthorized purpose, he could have made a hard copy and no one would have known. He apologized for his actions and was remorseful regarding his errors. Applicant testified that he and the CEO were friends and had a good relationship. He never shared the information with a subsequent employer or any person.[12]

It is unclear whether Applicant received any training on the appropriate handling of proprietary information while working for the company. In March and April 2014, he took it upon himself to complete training courses on Identifying and Safeguarding Personally Identifiable Information, Virtual Training for Security Professionals, and Facilities Security Officer Orientation for Non-Processing Facilities Curriculum. He testified he wanted to be part of the solution to ensure the proper handling of sensitive material.[13]

Applicant provided character letters that describe him as a loyal, ethical person who can be trusted. He has an in-depth understanding of the complexities associated with handling sensitive material and is greatly respected as one who goes to significant lengths to ensure compliance with the storage, transmission, and usage of such information. He is a diligent and conscientious professional.[14]

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.

[12] Tr. 128-129, 152-153.

[13] Tr. 129-131.

[14] AE C.

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 not drawn 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, 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. Such decisions entail a certain degree of legally permissible extrapolation of 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. The following are potentially applicable:

(a) illegal or unauthorized entry into any information technology system or component thereof; and

(e) unauthorized use of a government or other information technology system.

Applicant transferred the user names and passwords that gave him access to the company's business data from his company account to his personal account. He also transferred a business proposal, proprietary business data and the company's accounting guidelines to his personal account. He did this without authorization. I find the above disqualifying conditions apply.

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

(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.

I found Applicant's testimony and explanations for his actions to be credible. Applicant admitted he transferred the user name and password list he kept on his company computer to his personal computer. He did not separate the list between personal and business. I conclude this was an oversight by Applicant. However, he also intentionally transferred a user name and password that was given to him by Ms. W. This was unauthorized. The other transfers were also unauthorized, but Applicant did not have any nefarious intention to misuse this information. He intended to use this information to prepare for executing a contract that he would be working on, if approved, as a consultant with the company. He wanted to be ready so he could start right away. There is no indication he was using any information he transferred for any other purposes than to fulfill the work requirements as the program manager and consultant on the contract. He believed he was authorized to make the transfers, even though the evidence was to the contrary. When he learned of his mistake, he deleted all of the transferred data, apologized to the CEO, and took steps to ensure it would never happen again. I find his behavior happened under unusual circumstances, it is unlikely to recur, and it does not cast doubt on Applicant's current reliability, trustworthiness, and good judgment. No harm was done to the company. Although misguided, Applicant

believed he was acting in the best interests of his employer by preparing for the new contract. As soon as he became aware there was an issue he acted appropriately. I find all of the above mitigating conditions apply.

Guideline K, Handling Protected Information

AG ¶ 33 expresses the security concern pertaining to handling protected information:

> Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

AG ¶ 34 describes conditions that could raise a security concern and may be disqualifying. I have specifically considered the following:

> (b) collecting or storing classified or other protected information at home or in any other unauthorized locations;
>
> (d) inappropriate efforts to obtain or view classified or other protected information outside of one's need to know; and
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information.

Applicant admitted he used his company email account to transfer user names and passwords pertaining to proprietary business data and accounting policies. He did not have authorization to make these transfers and violated the company's rules and regulations. I find the above disqualifying conditions apply.

I have considered all of the mitigating conditions under AG ¶ 35, and I have specifically considered the following:

> (a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual currently reliability, trustworthiness, or good judgment; and
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities.

The mitigating condition analysis under Guideline M, use of information technology systems, is the same for Guideline K, handling protected information. I will not repeat the analysis, but include the following additional comments under this

guideline. Applicant mistakenly believed he was authorized to transfer the data. When he learned he was not, he immediately admitted his mistake and took corrective action by deleting all of the transfers. He has taken several courses to ensure he is aware of the rules and is in compliance. Applicant has exhibited a positive attitude toward the discharge of his duties relating to the protection of sensitive information and security responsibilities. I find the above mitigating conditions apply.

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):

> (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 have incorporated my comments under Guidelines M and K in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Applicant is 49 years old. He retired from the military after 20 years of honorable service. He made some mistakes after he resigned from working with Employer A. His actions were not intended to harm his former employer, but rather he was attempting to prepare for his new job as a consultant. Applicant believed he was authorized to make the transfers, but he did not have expressed approval from his supervisor. When he learned of his transgression, he immediately apologized and mitigated his conduct by deleting all of the transfers. His former CEO, who reported the conduct, believes Applicant is trustworthy and this was a one-time transgression. I believe it to be also. Overall, the record evidence leaves me without questions or doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the security concerns arising under the use of information technology systems guideline and the handling protected information guideline.

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 K:	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 a security clearance. Eligibility for access to classified information is granted.

_____
Carol G. Ricciardello
Administrative Judge