DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 07-11743
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Candace Le'i, Esquire, Department Counsel
For Applicant: Leslie McAdoo Gordon, Esquire

November 23, 2009

Decision

CURRY, Marc E., Administrative Judge:

Between May and August of 2005, Applicant abused his administrative privileges as a network analyst by accessing the e-mails of an employee of the Department of Defense without her knowledge or consent. Some of the e-mails were classified. This behavior generates security concerns under Guidelines E, personal conduct, M, misuse of information technology systems, and K, handling protected information. Applicant disclosed this adverse information to his current employer before beginning employment in October 2005. Since then, he has maintained a Top Secret clearance, and his on-the-job conduct and professionalism have been exemplary. Applicant has mitigated the security clearance concerns. Clearance is granted.

Statement of the Case

On April 9, 2009, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant detailing a security concern under Guidelines E, Personal Conduct, M, Misuse of Information Technology, and 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 revised adjudicative guidelines (AG) promulgated by the President on December 29, 2005, and effective within the Department of Defense for SORs issued after September 1, 2006.

Applicant answered the SOR on May 29, 2009, admitting all of the allegations except SOR ¶ 1.c. The case was assigned to me on July 28, 2009. On August 12, 2009, a notice of hearing was issued scheduling the case for September 9, 2009. The hearing was conducted as scheduled. I received 5 government exhibits, 10 Applicant exhibits, and the testimony of 4 Applicant witnesses. The transcript was received on October 17, 2009.

Findings of Fact

Applicant is a 32-year-old married man with three children ages 18, 13, and 12. He is a veteran of the United States Army where he served from 1995, directly after finishing high school, to 2003 when he was honorably discharged (Tr. 97). According to his supervisor during his last two years in the Army, he "demonstrated excellent performance in decision-making and pertinent information, and safeguard[ing] security" (Tr. 51). After leaving the Army, Applicant entered college, earning a bachelor's degree in computer systems in March 2008 (Tr. 99).

Shortly after leaving the military in 2003, Applicant began working for a defense contractor as a network administrator on classified systems (Tr. 98). Among other things, he managed the help desk. Also, when military clients were deployed abroad, Applicant was responsible for setting up their network systems at their respective duty stations (Tr. 123). In December 2004, Applicant held a part-time job with another defense contractor where he performed similar work (Exhibit 4 at 11; Tr. 108).

In late 2004, Applicant began working on the computer network of a female enlisted military member who had recently deployed abroad (Tr. 152). He performed this task through his primary employer. Although Applicant rarely saw the enlisted military member, they became friends. When she returned to the U.S. in January 2005, they became romantically involved (Tr. 122). Applicant did not tell her that he was married (Tr. 100).

In approximately April 2005, Applicant's girlfriend began to suspect he was married. After calling his home and speaking to his wife, she ended the relationship (Tr. 29). Applicant has not spoken with his ex-girlfriend since then (Tr. 101).

Applicant was concerned about his ex-girlfriend's well-being after their relationship ended (Tr. 118). In May 2005, he began accessing her work e-mails "to make sure [she] was okay" (Tr.118). His employer did not authorize him to read her e-mail, and she was unaware that he was accessing them (Exhibit 2 at 6). Some of the e-mails contained classified information (Answer at 1). Over the next three months,

Applicant accessed her e-mail approximately 25 times (Exhibit 2 at 6). At the time, Applicant held a Top Secret clearance with access to Sensitive Compartmented Information (SCI) (Tr. 104).

Applicant knew his conduct violated his company policies regarding the appropriate use of information systems (Tr. 105). Also, he knew that his conduct could result in his dismissal, if discovered (Answer at 1; Tr. 127).

Unbeknownst to Applicant, his ex-girlfriend had configured her e-mail to send electronic receipts to confirm that individuals whom she e-mailed had read her correspondence (*Id.*). In approximately September 2003, she received a return receipt from Applicant's e-mail address for a message that she did not send him (*Id.*). She became suspicious, and reported what she had learned to the agency's inspector general (*Id.*).

The agency's inspector general's office then conducted an investigation (*Id.*). On the afternoon of September 28, 2005, after confirming that Applicant wrongfully accessed the e-mails, an investigative agent questioned Applicant (Exhibit 2 at 6). Applicant admitted to the misconduct. Consequently, the agency then notified Applicant's employer, immediately revoked his SCI access, confiscated his badges, and escorted him from the building (Tr. 106). Earlier that day, Applicant had given his employer two-weeks notice of his resignation so that he could take a position with the company with whom he currently works (Exhibit 2 at 6). Applicant did not know he was under investigation when he resigned (Tr. 106). In an interoffice memo, a human resources representative from Applicant's ex-employer characterized the relationship between his resignation and the subsequent discovery of his misconduct as coincidental (Exhibit 3 at 4).

When Applicant returned home, he notified his part-time employer of the incident, and asked if he could still work there (Tr. 107). He had submitted his two-weeks notice to his part-time employer at the same time he had submitted it to his primary employer (*Id.*). His part-time employer refused his request, and allowed him to leave without working the last two weeks (*Id.*).

The facility security officer (FSO) of Applicant's current employer interviewed him in early October, as part of a routine background check (Tr. 70 - Testimony of FSO). At the time of the interview, the FSO had approximately 25 years of experience working in the defense security field (Tr. 70). The company's program manager had already extended Applicant a job offer (Tr. 72). Before the interview, the FSO performed a routine check of Applicant's security clearance history through the Department of Defense Security Service's Joint Personnel Adjudication System (JPAS). It revealed that Applicant's SCI had been revoked, and that he retained a Top Secret clearance (Tr. 75). When the FSO asked about the circumstances surrounding the revocation of his SCI access, Applicant discussed it honestly and remorsefully (Tr. 75, 79).

The FSO was perplexed as to how Applicant lost his SCI access, but retained his Top Secret clearance (Tr. 77). He testified to the following conversation with a DSS representative:

> I said, 'I've spoken to the Program Manager, and they want to hire this individual, but I'm leery about hiring him, because if we hire him, will they turn around in 30 days based on this event and pull his clearance?'
>
> And they said, . . . 'anything can happen tomorrow or the next day, but as of today, he is a cleared individual who can be hired and use his Top Secret clearance . . .' (Tr. 78).

The FSO then went to the company president and told her that "the government has chosen not to pull Applicant's Top Secret clearance, [and he was not] in a position right now . . . to think that [Applicant] could be . . . put in a position to compromise his clearance information" (Tr. 79).

Applicant was then hired for a one-year probationary period (Tr. 77). During this period, the FSO closely monitored him, speaking to the program manager quarterly, and observing his work relationships (Tr. 80, 82). Applicant successfully completed the probationary period (Tr. 81). Also, he has completed multiple security trainings over the past four years (*see generally*, Exhibit H). In sum, he has demonstrated "impeccable character and security awareness" since working for his current employer (Tr. 83).

Applicant has completely rebuilt his wife's level of trust with him (Tr. 32). She characterized their current relationship as "great" (Tr. 32).

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the revised adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful 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. 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."

Under Directive ¶ E3.1.14, the government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, Applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." Applicant has the ultimate burden of persuasion as to obtaining a favorable security decision.

Analysis

Guideline E, Personal Conduct

Under this guideline, "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" (AG ¶ 15).

Applicant while serving the Department of Defense as a network analyst had an affair with a woman whom he met while installing her information systems network as part of his job duties. After she ended the affair, he abused his network privileges by accessing her e-mails without her permission or his employer's authorization, on 25 occasions. AG ¶ 16(e), "personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as . . . engaging in activities which, if known, may affect the person's personal, professional, or community standing," applies.

Applicant's contention that his resignation from his employer was unrelated to their discovery of his misconduct is supported by his ex-employer's internal memoranda that the government submitted. I conclude that he did not resign from his employment in lieu of being fired, as alleged in SOR subparagraph 1.c. I resolve SOR 1.c in Applicant's favor.

Applicant's inappropriate workplace behavior calls into question his trustworthiness. However, I decline to apply AG ¶ 16(d)(1), "untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information," or AG ¶ 16(d)(2), "disruptive, violent, or other inappropriate behavior in the workplace," or AG ¶ 16(d)(4), "evidence of significant misuse of Government or other employer's time or resources."All of these factors accurately characterize his conduct; however, their applicability under Guideline E is predicated on Applicant's conduct not being "explicitly covered under any other guideline" (AG ¶ 16(d)). Applicant's conduct is covered under both Guidelines M, Use of Information Technology Systems (AG ¶¶ 39-41), and K, Handling Protected Information, (AG ¶¶ 33-35), rendering their discussion under these particular Guideline E disqualifying conditions superfluous.

Applicant reconciled with his wife. He has not engaged in additional episodes of adultery. His current employer was aware of the conduct when it hired him. Applicant discussed the incident comprehensively and remorsefully with his current employer's

FSO, who then recommended his hiring, after confirming with DSS that he still retained a Top Secret clearance. In the four years since working for his current employer, he has completed multiple security trainings, and has demonstrated outstanding character and security awareness. 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 17(e), "the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress," apply.

Guideline M, Use of Information Technology Systems

The security concern under this guideline is set forth in AG ¶ 39 as follows:

> 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. Information technology systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

As a network administrator with special access for troubleshooting or monitoring his company's information security systems, Applicant was a "privileged user" under the National Industrial Security Program Operating Manual[1] (NISPOM). Applicant abused his privileged user status, and violated company policy by viewing his ex-girlfriend's e-mail without her knowledge or consent. Consequently, AG ¶¶ 40(a), "illegal or unauthorized entry into any information system or component thereof," and 40(e), "unauthorized use of a government or other information technology system," apply.

Applicant's misconduct occurred four years ago and has not recurred. His current employer is pleased with his work performance and adherence to security standards. 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," applies.

Guideline K, Handling Protected Information

Under this guideline, "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 ¶ 33). Applicant accessed his ex-girlfriend's e-mail without authorization. Some of the e-mails Applicant accessed

[1]DoD 5220.22-M, ¶ 8-105.

without authorization contained classified information of which he had no need to know. AG ¶ 34(d), "inappropriate efforts to obtain or view classified or other protected information outside one's need-to-know," applies. Applicant also violated the NISPOM's requirement for privileged information system users to "be accountable for their actions" on an information system (¶ 8-105c.(3)).

Applicant has not committed any security violations in four years. He has completed multiple security trainings, and displays an outstanding attitude toward security awareness. AG ¶¶ 34(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," and 34(b), "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities," 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 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."

Applicant's misconduct breached his wife's trust, his employer's trust, and the federal government's trust when he engaged in an affair with a government employee, then abused his networking privileges to furtively monitor her e-mail. Applicant had never engaged in similar conduct in the past, and it has not recurred. His current employer is highly pleased with his work performance and security awareness. Applicant has successfully completed multiple security trainings, and enrolled in college earning a degree in information systems in 2008. Also, he has repaired his relationship with his wife. The seriousness of Applicant's conduct is outweighed by the presence of rehabilitation and the amount of time that has elapsed since its occurrence. Under these circumstances, the likelihood of recurrence is minimal. Upon considering the applicable disqualifying and mitigating conditions together with the whole person concept, I conclude Applicant has mitigated the 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 E:	FOR APPLICANT
Subparagraph 1.a - 1.e:	For Applicant
Paragraph 2, Guideline M:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3, Guideline K:	FOR Applicant
Subparagraph 3.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.

MARC E. CURRY
Administrative Judge