DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	
SSN: ----------	)	ISCR Case No. 06-23351
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Melvin Howry, Esquire, Department Counsel
For Applicant: *Pro se*

November 19, 2010

Decision

LYNCH, Noreen, Administrative Judge:

On November 27, 2009, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) alleging facts which raise security concerns addressed in the adjudicative guidelines (AG) under Guideline M (misuse of information technology), Guideline E (personal conduct), and Guideline J (criminal conduct). DOHA acted 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).
.

Applicant timely responded to the SOR, denied all allegations in the SOR with explanation, and requested a hearing. DOHA assigned the case to me on July 26, 2010. DOHA issued a Notice of Hearing on September 10, 2010. Department Counsel offered four exhibits, which were admitted without objection as Government Exhibits (GE) 1-4. Applicant testified and presented eight exhibits, which were admitted without objection as Applicant Exhibits (AE) A-H. DOHA received the transcript (Tr.) On October 18, 2010. Based upon a review of the case file, pleadings, exhibits, and testimony, eligibility for access to classified information is granted.

Findings of Fact

Under Guideline M, the government alleged in SOR ¶ 1.a that Applicant intentionally used (reconfigured and installed) a wireless router that exceeded authorized access to the internet computer networks in about November or December 2003, while employed with a defense contractor. In SOR ¶ 1.b, the government alleged in about December 2003, Applicant was investigated by the Office of the Inspector General and found in violation of SSC-Network Policy, section 4.3.3, "Wireless Devices" and 18 U.S.C. Section 1030, "Fraud and Related Activity in Connection with Computers".

Under Guideline E, the government alleged in SOR ¶ 2.a the same information alleged in SOR ¶ 1.a and 1.b.

Under Guideline J, the government alleged in SOR ¶ 3.a the same information as alleged in SOR ¶ 1.a. In SOR ¶ 3.b the government alleged that information alleged in SOR ¶ 1.b constitutes a violation of Federal law, Title 18 U.S.C. Section 1001, a felony. After a thorough review of the pleadings, and exhibits, I make the following findings of fact.

Applicant is 37 years old. Applicant served in the U.S. military from 1991 until 1996, and held a security clearance since approximately 1995. (GE 1) He graduated from college in 2001, and received his Master of Business Administration degree in 2007 (AE E). He is divorced and has no children. (Tr. 23)

Applicant has worked as an engineer (civilian employee) since approximately 1997 various contractors. He is currently a key management employee of his own company. (Tr. 24) The company is a service-disabled veteran-owned company. (AE C).

In December 2003, while employed with a defense contractor, Applicant installed a wireless router in a cubicle space based on the request of Applicant's co-worker, who was a government employee. Applicant's co-worker purchased the router because the personnel working in that area could not access network resources to accomplish their jobs. (GE 1)

On December 31, 2003, a report of a suspicious person outside the military compound that may have been trying to gain access or gain a signal from a government agency came to light. The report of the incident led to an inspection of the work area where Applicant and his co-worker had installed the wireless router. In January 2004, the router was discovered. Applicant's employer removed the router. At the time, Applicant was on vacation.

Applicant was interviewed concerning the installation of the wireless router and about the location of the wireless router. Applicant explained that he found an elevated place between cubicles and that there was no other place that would work quite as well. He explained he was not aware of any policy that prohibited the installation of a wireless router. He also acknowledged that was not a good excuse. He also stated that the

router gave him access to the same resources (files) that he had already been allowed to access. (Tr. 37) The interviewer's comment was "that Applicant's explanation was not persuasive." Applicant further explained that he did what he thought necessary by setting an encryption feature on the device so all wireless traffic to and from the device would be secured. (GE 1)

An investigation conducted by Applicant's employer resulted in a report generated in July 2004. The report revealed that Applicant's government co-worker showed poor judgment by asking Applicant to install and reconfigure a wireless router. Applicant's co-worker knew or should have known that this was against policy and put Applicant in "an unacceptable position." It clearly noted that Applicant acted on the request and advice of the long-term government employee. However, Applicant as an engineer in the filed "showed a lack of concern for the network and information technology systems security." He did not show due diligence in protecting the wireless access point itself, its wireless clients, and ultimately the command network.

Persons who are found to be involved in "exceeding unauthorized access" to a computer or network may be prosecuted under 18 U.S.C. Section 1030, "Fraud and Related Activity in connection with Computers," which is a felony charge. The incident in this case was referred to the U.S. Attorney's Office for potential prosecution. (GE 4)

As a result of the investigation, Applicant was reprimanded by his employer. He was advised that there would be no criminal prosecution. The report noted that the agency has not finalized a regulation addressing wireless security policy. Since its establishment in 2001, however, wireless security policy for the SSC has been clearly delineated and readily available on the command Intranet.

Applicant was candid and forthcoming at the hearing. He was credible in his explanation of the events that occurred. He was asked to help his government co-worker, who had been working there for 20 years, solve a problem and he offered to install the wireless router. The co-worker did not express knowledge of network security policy. Applicant received good evaluations that year and continued to work in that capacity until 2006. (Tr. 76)

Applicant submitted ten letters of recommendation from supervisors and colleagues from 1992 until 2006. Each describes him as a person of excellent character. He is professional and tenacious. He possesses expert knowledge. Former program managers describe Applicant as a person who is an enthusiastic engineer with excellent communication skills. He is a joy to work with. Applicant is detail oriented and determined. He is a critical member of the team. He delivered extraordinary technical support and management expertise to the program. Applicant resolves problems quickly. He has demonstrated a rare combination of exceptional technical skill, innovative problem solving and superior organizational skills that have led directly to the success in the project. He understands the technical issues and the military organization and environment. (AE D)

Applicant earned awards and letters of appreciation during his military career. He graduated from a specialized manager course with distinction. He is and has maintained strict responsibility and accountability for a great deal of secret information.

Applicant acknowledged that in retrospect, he should have received written permission from someone in the government before installing a wireless router. However, he was trying to help his "customer" and to provide service. He had no malicious intent in the use of the wireless router. He realizes that he should have researched the issue to find specific policies that were applicable. Applicant testified credibly that at the time he was not aware of the existing policy section affecting wireless routers (4.3.3). He admitted that he learned a lesson from the incident and that he is sure it will not happen again.

Policies

Each security clearance decision must be a fair, impartial, and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the adjudicative guidelines (AG).[1] Decisions must also reflect consideration of the factors listed in ¶ 2(a) of the AG.[2] The presence or absence of a disqualifying or mitigating conditions is not determinative of a conclusion for or against an applicant. However, specific applicable guidelines must be followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of a clearance. In this case, the pleadings and the information presented by the parties require consideration of the security concerns and adjudicative factors addressed under Guideline M (misuse of information technology systems), at AG ¶ 39, Guideline E (personal conduct) at AG ¶ 15, and Guideline J (criminal conduct) at AG ¶ 30.

A security clearance decision is intended to resolve whether it is clearly consistent with the national interest[3] for an applicant to either receive or continue to have access to classified information. The government bears the initial burden of producing admissible information on which it based the preliminary decision to deny or revoke a security clearance for an applicant. Additionally, the government must be able to prove controverted facts alleged in the SOR. If the government meets its burden, it then falls to the applicant to refute, extenuate or mitigate the government's case. Because no one has a right to a security clearance, an applicant bears a burden of

[1] Directive. 6.3.

[2] Commonly referred to as the "whole person" concept, these factor are: (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.

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

persuasion.[4] A person who has access to classified information enters into a fiduciary relationship with the government based on trust and confidence. The government, therefore, has a compelling interest in ensuring each applicant possesses the requisite judgement, reliability and trustworthiness of one who will protect the national interests. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the government.[5]

Analysis

Misuse of Information Technology Systems.

Under Guideline M, "[n]oncompliance 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." (AG ¶ 39). Applicant acknowledged that in 2003, he installed and reconfigured a wireless router which exceeded authorized access to a government classified network. The information requires consideration of the disqualifying conditions listed at AG ¶ 40(a) (*illegal or unauthorized entry into any information technology system or component thereof*); AG 40(c) (*use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system*); AG ¶ 40(e) (*unauthorized use of a government or other information technology system*) and ¶ 40(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*).

I find that AG ¶¶ 40(a), 40(c), 40(e), and 40 (f) apply because a router is an information technology system that was used to gain unauthorized access to a classified network in violation of information technology rules, procedure, or guidelines.

The record supports consideration of Guideline M mitigating conditions listed in AG ¶ 41. This conduct occurred in December 2003. Applicant explained that he was requested to install the router purchased by his government co-worker to help alleviate a situation. He complied with the request. He was not aware of a policy that prohibited the wireless router. He used means to encrypt the system. He believed this would allow a more efficient use of time. Applicant was on vacation and when he returned the wireless router was confiscated. He cooperated with the investigation. He was counseled or reprimanded by his employer. He continued to work as a contractor and he received letters of appreciation for his work. He then read the relevant policy. He now realized that it was imprudent to follow the request of his government co-worker without researching the issue and obtaining approval. Applicant has held a security

[4] *See Egan,* 484 U.S. at 528, 531.

[5] *See Egan;* Revised Adjudicative Guidelines, ¶ 2(b).

clearance during his Navy service and as a contractor without any other incident. (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. The other mitigating conditions are not applicable.

Personal Conduct.

The security concern about Applicant's personal conduct, as expressed in the AG ¶ 15, is that "[c]onduct 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."

As to SOR ¶ 2.b, available information requires consideration of the disqualifying conditions listed in AG ¶ 16(d)(4) (*evidence of significant misuse of Government or other employer's time or resources)* and AG ¶ 16(e)(1) (*personal conduct, or concealment of information about ones' 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*). Certainly, Applicant's violation of company policy by unauthorized installation of a router over a sensitive network is conduct a person might wish to conceal, as it adversely affects a person's professional and community standing.

The mitigating conditions outlined in 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 it 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*) apply. Applicant acknowledged that he installed the wireless router as discussed above under Guideline M. This incident occurred in 2003. Applicant has held a security clearance for many years. He cooperated with the investigation after the complaint was made. He did not alert his employer because he was on vacation and the router was already confiscated when he returned to work. Applicant takes responsibility for his actions.

Criminal Conduct.

The security concerns about Applicant's criminal conduct, as expressed in the AG ¶ 30, is that "criminal activity creates doubt about a persons' judgment, reliability, and trustworthiness, By its very nature, it calls into question a persons's ability or willingness to comply with laws, rules and regulations."

AG ¶ 31(a) (a single serious crime or multiple lesser offense*)* is an applicable disqualifying condition.

AG ¶ 31(c) (allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted*)* is an applicable disqualifying condition*.* However, after an investigation, never presented to the U.S. Attorney's Office, the office did not prosecute Applicant. Applicant was reprimanded by his employer for the installation of the wireless router. He read the applicable policy after the incident and then complied with the policy.

Title 18, U.S.C. Section 1030 requires "intent to defraud, reckless damage or intent to extort among other things. In this case, Applicant did not present the required intent. Thus, he is not in violation of the statute.

An applicant might be able to mitigate Guideline J security concerns. One such mitigating condition (*so much time has elapsed since the criminal 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 ¶ 32(a) may apply. For the reasons discussed above, I do not believe Applicant would compromise national security to avoid public disclosure of the incident. Any criminal conduct security concerns pertaining to the incident are dealt with more thoroughly under Guideline M and Guideline E in this decision. Criminal conduct security concerns are mitigated.

Whole- Person Concept.

I have evaluated the facts presented in this record and have applied the appropriate adjudicative factors, pro and con, under Guidelines M, E, and J. I have also reviewed the record before me in the context of the whole-person factors listed in ¶ AG 2(a).[6] Applicant is a mature adult who served in the military. He held a security clearance for many years. However, when working for a defense contractor in 2003, he installed a wireless router at the request of a government employee in violation of a policy against such wireless routers. He acknowledges his mistake and is sorry for the incident. The positive information about Applicant is sufficient to overcome the adverse information about his conduct at his previous job under Guideline M and Guideline E. This does not raise doubts about his reliability and trustworthiness. He has mitigated the security concerns under the above-referenced guidelines.

Formal Findings

Formal findings 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
Subparagraph 1.b:	For Applicant

[6] *See* footnote 2, *supra.*

Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3, Guideline J:	FOR Applicant
Subparagraph 3.a-3b:	For Applicant

Conclusion

In light of all of the foregoing, it is clearly consistent with the national interest to grant Applicant access to classified information. Clearance granted.

NOREEN A. LYNCH
Administrative Judge