KEYWORD: Personal Conduct; Information Technology

DIGEST: Applicant is a 37-year-old employee of a defense contractor. In December 2005, Applicant hacked into a former employer's data network and disabled the company's phone system. Applicant regretted his actions, informed the company, made restitution, and is receiving psychiatric treatment. He has not mitigated the security concerns raised by his actions. Clearance is denied.

CASENO: 06-23182.h1

DATE: 06/14/2007

DATE: June 14, 2007

| | | |
|---|---|---|
| In re: | ) | |
| | ) | |
| ---------- | ) | ISCR Case No. 06-23182 |
| SSN: ---------- | ) | |
| | ) | |
| Applicant for Security Clearance | ) | |

**DECISION OF ADMINISTRATIVE JUDGE**
**EDWARD W. LOUGHRAN**

**APPEARANCES**

**FOR GOVERNMENT**
Francisco Mendez, Esq., Department Counsel

**FOR APPLICANT**
Leslie McAdoo, Esq.

**SYNOPSIS**

Applicant is a 37-year-old employee of a defense contractor. In December 2005, Applicant hacked into a former employer's data network and disabled the company's phone system. Applicant

regretted his actions, informed the company, made restitution, and is receiving psychiatric treatment. He has not mitigated the security concerns raised by his actions. Clearance is denied.

## STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. On January 30, 2007, DOHA issued a Statement of Reasons[1] (SOR) detailing the basis for its decision–security concerns raised under Guideline E (Personal Conduct) and Guideline M (Use of Information Technology Systems) of the revised Adjudicative Guidelines (AG) issued on December 29, 2005, and implemented by the Department of Defense for SORs issued after September 1, 2006. The revised guidelines were provided to Applicant when the SOR was issued. Applicant answered the SOR in writing on February 21, 2007, and elected to have a hearing before an administrative judge. The case was assigned to me on April 4, 2007. A notice of hearing was issued on April 12, 2007, scheduling the hearing for May 17, 2007. The hearing was conducted as scheduled to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The Government offered two exhibits that were marked as Government Exhibits (GE) 1 and 2, and admitted without objections. Applicant testified and offered 17 exhibits that were marked Applicant Exhibits (AE) A through Q, and admitted without objections. DOHA received the hearing transcript (Tr.) on May 25, 2007.

## FINDINGS OF FACT

Applicant's admissions to the allegations in the SOR are incorporated herein. In addition, after a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is a 37-year-old employee of a defense contractor. He is single with no children. Applicant is a college graduate.[2]

Applicant worked for his former employer from September 1998 to August 2005. He was an IT Systems Engineer when he voluntarily left the company to work for his current employer. After he was with his current employer for several months, Applicant started to regret leaving his former company. Applicant began negotiating with his former company for him to return to work for them. After some discussions, the talks stalled.[3]

Before he left his former company, Applicant copied their electronic data, including passwords for their systems. On about December 23, 2005, Applicant gained access to his former employer's data network via his home computer through a hole in their system's firewall, using the information and passwords he kept after he left the company. Applicant disabled an interface in their system, which Applicant knew would cause disruption to their network. Applicant shut down the company's phone system so that they could not take incoming or make outgoing phone calls. The

[1]Pursuant to Exec. Or. 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended (Directive).

[2]Tr. at 85; GE 1.

[3]Tr. at 86-90; GE 1; AE C.

company retained a consultant to correct the system, and it caused their employees to expend many hours in their attempt to correct the problem.[4]

Applicant regretted his actions and accessed the system again several days later in order to correct the damage he caused the company, but the company had already remedied the situation. On about January 4, 2006, Applicant contacted his former company and admitted the actions he took. On May 10, 2006, Applicant acknowledged in writing to his former company what he did to their system, and he paid the company $2,000 to reimburse them for their costs incurred in correcting the problem.[5]

Applicant testified that he hacked into his former company's system because he thought the company might contact him to help correct the system, and he could "show them that they actually needed me."[6]

Applicant discussed the electronic intrusion into his former company's system when he was interviewed pursuant to his background investigation on September 10, 2006.[7]

A forensic psychiatric examination of Applicant was conducted by a psychiatrist on April 12, 2007. The psychiatrist testified during the hearing. He has a background that includes national security issues, and was accepted as an expert in forensic psychiatry. Applicant was diagnosed as suffering from attention deficit disorder, about which Applicant was unaware. He was also found to be "suffering from intermittent depression, anxiety, and sociophobia which are disorders grounded in some latent problems of adulthood, and from traumas sustained by him in his adolescent high school years."[8] His problems are related to some significant self-esteem problems. Applicant has weight problems which affected his body image and his personal image of himself. He is also psychologically immature, and much of his emotional psychological development is suspended at the adolescent stage of development. The psychiatrist believes Applicant's immaturity clearly contributed to his acts against his former employer.[9]

The psychiatrist found and testified that Applicant's problems are very treatable and that his prognosis is good with treatment. He further found that it is unlikely Applicant will repeat such an act, particularly if he accepts and obtains appropriate and recommended treatment for his problems.

---

[4]Tr. at 88-91, 106-116, 120-121; AE H.

[5]Tr. at 91-94; AE H.

[6]Tr. at 94.

[7]Tr. at 100-101; GE 2; AE F.

[8]AE J at 4.

[9]Tr. at 25-82; AE I, J.

He found no indications that Applicant would willfully and intentionally compromise the security of the United States.[10]

Applicant is now receiving treatment from a clinical psychologist. The psychologist for the most part agrees with the psychiatrist's diagnosis, and that treatment for six to twelve months seems reasonable. The psychologist also recommends a psychiatric evaluation for possible antidepressant medication. Applicant was scheduled to meet a treating psychiatrist the day after the hearing.[11]

Applicant has informed his current employer about what he did to his former employer. His supervisor wrote a letter on his behalf, acknowledging that Applicant informed her of his actions against his former employer. She cited his trustworthiness, intelligence, honesty, diligence, professionalism, dedication, security awareness, and respect for security rules and procedures. She stated his judgment in this incident was unquestionably poor, but believes it was a single mistake, and recommends him for a security clearance.[12]

Applicant's performance evaluations from both his current and former companies are excellent.[13] Applicant submitted additional character letters from people who know him from both his current and former companies, as well as people who know him personally. All are aware of Applicant's actions. All were surprised by his actions and consider it a one-time event. They state Applicant is honest, trustworthy, professional, forthright, loyal to this country, with a tremendous amount of integrity, and a man of principle. They all recommend Applicant for a security clearance.[14]

## POLICIES

"[N]o one has a 'right' to a security clearance."[15] As Commander in Chief, the President has "the authority to . . . control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position . . . that will give that person access to such information."[16] The President authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so."[17] An applicant has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his or her security clearance. The clearly consistent standard indicates that security clearance determinations

---

[10] *Id.*

[11] Tr. at 103-104; AE Q.

[12] Tr. at 122-123; AE K.

[13] AE B, D, E.

[14] AE L-P.

[15] *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

[16] *Id.* at 527.

[17] Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960).

should err, if they must, on the side of denials.[18] Any reasonable doubt about whether an applicant should be allowed access to sensitive information must be resolved in favor of protecting such sensitive information.[19] The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of an applicant. It is merely an indication that the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.[20]

The revised Adjudicative Guidelines set forth potentially disqualifying conditions (DC) and mitigating conditions (MC) under each guideline. Additionally, each security clearance decision must be a fair and impartial commonsense decision based on the relevant and material facts and circumstances, the whole-person concept, along with the adjudicative process factors listed in the Directive and AG ¶ 2(a).

Conditions that could raise a security concern and may be disqualifying, as well as those which would mitigate security concerns, are set forth and discussed in the conclusions section below.

## CONCLUSIONS

I have carefully considered all the facts in evidence and the legal standards discussed above. I reach the following conclusions regarding the allegations in the SOR.

**Guideline M: 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 reliability and trustworthiness, calling into question the willingness or ability to 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.

Based on all the evidence, Use of Information Technology Systems Disqualifying Condition (UITS DC) 40(a) (*illegal or unauthorized entry into any information technology system or component thereof*), UITS DC 40(b) (*illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system*), UITS DC 40(c) (*use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system*), and UITS DC 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*) all apply in this case.

[18]ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002).

[19]*Id*.; Directive, ¶ E2.2.2.

[20]Exec. Or. 10865 § 7.

I have considered all the Use of Information Technology Systems Mitigating Conditions (UITS MC), and I especially considered UITS MC 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*). Applicant's conduct was very serious and recent, and it casts doubt on his reliability, trustworthiness, and good judgment. Applicant's psychiatrist believes his psychological issues contributed to his conduct. Those psychological issues are only beginning to be addressed. I am unconvinced that this type of conduct will not recur. Applicant has not established UITS MC 41(a).

**Guideline E: Personal Conduct**

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. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The potential Personal Conduct Disqualifying Condition (PC DC) in this case is PC DC 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 . . .* ).

Applicant's electronic intrusion into his former company's system, and disabling of their telephone service is conduct which could affect Applicant's personal, professional, and community standing. PC DC 16(e) is established.

I have considered all the Personal Conduct Mitigating Conditions (PC MC), and I especially considered PC MC 17(c) (*the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment*), PC MC 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 PC MC 17(e) (*the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress*).

As discussed above under the mitigating condition applicable under Guideline M, I find Applicant's conduct to be very serious and recent. It casts doubt on his reliability, trustworthiness, and good judgment. While he only disrupted the system once, and he is now receiving counseling and treatment, I am not convinced that it is unlikely to recur. PC MC 17(c) and PC MC 17(d) are not applicable.

Applicant informed his former company of his actions and made restitution. He also informed friends, associates, and his current company, and they continue to support him. That has reduced Applicant's vulnerability to exploitation, manipulation, and duress. PC MC 17(e) is applicable.

**Whole Person Analysis**

The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating Applicant's case, I have considered the adjudicative process factors listed in the Directive and AG ¶ 2(a). I have also considered every finding of fact and conclusion discussed above.

I considered the favorable character evidence, and the evidence presented from the forensic psychiatrist and Applicant's clinical psychologist. The psychiatrist testified he did not believe that as Applicant goes through treatment and addresses the problem, that he is at risk of doing something like this again. He based that on Applicant's behavior pattern throughout his lifetime, and the fact that he only did this once. He stated "the best predictor of behavior is previous behavior."[21] Applicant hacked into his former employer's system and shut down their phone system. That is an inexcusable action that reflected directly on Applicant's judgment, honesty, reliability, trustworthiness, and willingness to comply with rules and regulations. Other than an actual security violation, this is the type of action that causes the greatest concern, and is hopefully preventable through the security screening process. I agree with the psychiatrist that previous behavior is the best predictor of behavior. In this case, Applicant's previous behavior of hacking into his former company's system is so serious that it would be imprudent to grant Applicant a security clearance. To do so would risk Applicant committing similar behavior, with grave implications to national security, because this time we would have given him access to classified information or systems. The acceptance of such a risk would not be clearly consistent with the national interest.

After weighing the disqualifying and mitigating conditions and evaluating all the evidence in the context of the whole person, I conclude Applicant has mitigated the security concerns based on his personal conduct. He has not mitigated the security concerns based on his use of information technology systems.

## FORMAL FINDINGS

The following are my conclusions as to each allegation in the SOR:

| | |
|---|---|
| Paragraph 1. Guideline E: | FOR APPLICANT |
| Subparagraph 1.a: | For Applicant |
| Paragraph 2. Guideline M: | AGAINST APPLICANT |

[21] Tr. at 55.

Subparagraph 2.a: Against Applicant

## DECISION

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant or continue a security clearance for Applicant. Clearance is denied.

Edward W. Loughran
Administrative Judge