DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 08-08632
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Richard Stevens, Esquire, Department Counsel
For Applicant: *Pro se*

March 25, 2011

Decision

HENRY, Mary E., Administrative Judge:

After a review of the pleadings, exhibits, and testimony, questions or doubts as to Applicant's eligibility and suitability for a security clearance remain, as he has not mitigated the Government's security concerns. Applicant's eligibility for access to classified information is denied.

Applicant signed an Electronic Questionnaire for Investigations Processing (e-QIP) version of a security clearance application (SF-86) on August 10, 2007. The Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) on July 30, 2010, detailing security concerns under Guideline E (Personal Conduct), Guideline M (Use of Information Technology Systems), and Guideline K (Handling Protected Information), that provided the basis for its preliminary decision to deny him a security clearance. 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 For Determining Eligibility for Access to Classified Information (AG) implemented on September 1, 2006.

Applicant acknowledged receipt of the SOR on August 11, 2010. He answered the SOR in writing on August 25, 2010. Applicant requested a decision on the record. However, pursuant to Paragraph E3.1.7. of the Additional Procedural Guidance of Enclosure 3 of the Directive, Department Counsel requested a hearing before an administrative judge on September 28, 2010. (Hearing Exhibit 1) Department Counsel was prepared to proceed on October 28, 2010, and I received the case assignment on November 3, 2010. DOHA issued a notice of hearing on November 12, 2010, and I convened the hearing as scheduled on December 16, 2010. The Government offered exhibits marked as GE 1 through 14, which were admitted into evidence without objection. Applicant testified and submitted exhibits marked as AE A through E, which were admitted into evidence without objection. I held the record open until December 23, 2010, for Applicant to submit additional matters. Applicant timely submitted AE F through AE I without objection.[1] The record closed on December 23, 2010. DOHA received the transcript of the hearing (Tr.) on December 28, 2010.

Procedural Ruling

Motion to Amend the SOR

At the end of the hearing, Department Counsel moved to amend allegation 1.b of the SOR to conform with the hearing testimony. Specifically, Department Counsel asked to change the words "company laptop" to "personal laptop." Applicant did not object to amending the SOR. (Tr. 129-131) The Motion to Amend was granted, and allegation 1.b of the SOR was changed as requested.

Findings of Fact

In his Answer to the SOR, Applicant admitted the factual allegations in ¶¶ 1.c, 1.d, and 1.e of the SOR. His admissions are incorporated herein as findings of fact. He denied the factual allegations in ¶¶ 1.a and 1.b of the SOR.[2] He did not admit or deny the allegations in SOR paragraphs 2.a (Guideline M) and 3.a (Guideline K). His failure is

[1]AE F and AE G are letters of congratulations from 2005. AE H contains Applicant's awards from 2005 and 2006, while working overseas in or near a war zone. AE I contains information on a communications system conceived by the Applicant and in use by the military.

[2]When SOR allegations are controverted, the Government bears the burden of producing evidence sufficient to prove controverted allegations. Directive, ¶ E3.1.14. "That burden has two components. First, the government must establish by substantial evidence that the facts and events alleged in the SOR indeed took place. Second, the government must establish a nexus between the existence of the established facts and events and a legitimate security concern." *See* ISCR Case No. 07-18525 at 4 (App. Bd. Feb. 18, 2009), (concurring and dissenting, in part) (citations omitted). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 08-06605 at 3 (App. Bd. Feb. 4, 2010); ISCR Case No. 08-07290 at 2 (App. Bd. Nov. 17, 2009).

deemed a denial of these allegations. He also provided additional information to support his request for eligibility for a security clearance. After a complete and thorough review of the evidence of record, I make the following additional findings of fact.

Applicant, who is 55 years old, works as a communications engineer for a Department of Defense contractor. He began his current employment with this contractor in January 2004.[3] He is chief of his communications engineering department and holds a fellowship position with his employer, as he is an expert in his are of communications. His employer states that he is a very talented and experienced engineer, and rated him as an exceptional contributor in his most recent evaluation. His evaluations for the last six years have rated him as high contributor or exceptional.[4]

From 2004 through 2006, Applicant, a civilian, worked overseas, in or near the Iraq war zone. While overseas, he received several awards and other recognition for his technical excellence and work performance. Through his ideas and abilities, he also contributed significantly to the development of a communications systems now used by the military. He served in the military reserves and on active duty for 12 years, from December 1979 through May 1985 and April 1987 through November 1993. Applicant held a security clearance during his military duty and after his military service. There is no evidence that he mishandled classified information or violated the rules for handling classified information at any time.[5]

Applicant married in 1977. He has two sons, who are now 29 and 24 years old. He attended college and earned an associate's degree. He taught himself many of his current skills. He holds industry and Federal Communications Commission licenses in communication infrastructure. Since 1997, Applicant has worked in his area of communications expertise.[6]

In 1986, Applicant worked for the local police department in a rural town. He also started and operated a part-time radio business, which eventually included two partners, who were the local Chief of Police and a councilman. His communications business received used radio items from the police department and a variety of other communications equipment from different sources. In April 1986, Applicant arrived at work to find that someone had broken into the radio shop and taken one item. He reported the break-in to the police, who investigated. The local police determined that the burglary appeared to be an inside job and identified a suspect, who was an employee of the radio shop. The employee-suspect told the local police that Applicant and he stole mobile radio units from cars in the local area and that Applicant most likely

[3]Applicant worked for this company from 1997 until 2000 and held a security clearance while employed. GE 1.

[4]GE 1; AE B; AE C; Tr. 35.

[5]GE 1; AE E - AE I.

[6]GE 1; Tr. 35, 37-39.

disposed of the items stolen in the burglary in April 1986.[7] During the investigation, the local police found five federal interceptor sirens from an out-of-state police department, which had been given to the Applicant by a police officer from the out-of-state police department. Because the Federal Bureau of Investigation (FBI) was conducting an investigation on the interstate transportation of stolen property, the local police contacted the FBI. The FBI investigated Applicant. The FBI contacted the out-of-state police officer, who confirmed that he and Applicant traded communications equipment, as the police officer also had a communication equipment business, and that he mistakenly shipped Applicant the sirens. A month after their initial investigation, the local police searched Applicant's business and seized several items with missing serial numbers, including a radio reported stolen in another state. The police arrested Applicant following their search and seizure.[8]

At the conclusion of the FBI investigation, the federal prosecutor declined to proceed in court. The State, however, indicted Applicant on 12 counts of criminal use of article with altered identification mark because the serial number had been removed on various equipment found in his business shop. The indictment does not indicate if the crimes for which Applicant was charged were misdemeanors or felonies, although the FBI criminal records report does indicate at least one charge was a felony offense. In 1988, the state filed a motion for *Nolle Prosequi*, which the court granted on August 19, 1988. The record contains no additional evidence of criminal conduct. Applicant did not list his felony arrest on his SF 86.[9]

In his first statement to the Office of Personnel Management (OPM) investigator on February 19, 2009, Applicant discussed the radio communications business he operated. He acknowledged being arrested for no serial numbers on walkie-talkies, then indicated he was released a few hours later because the radio company told the police that the walkie-talkies were a gift. When asked by the investigator about why he failed to list his 1986 arrest, he stated that he misunderstood the question. He thought the question asked if he had ever served a sentence for a crime he committed.[10]

Applicant met with the OPM investigator a second time on April 1, 2009 to discuss charges listed on the FBI criminal records report. Specifically, they discussed the 1986 charges of receiving stolen property from another state, severity unknown; criminal use of an article with an altered identification mark, a felony; and acquiring a license plate for the purpose of concealing the identification of a motor vehicle, a misdemeanor. Applicant told the OPM investigator that the charge of receiving stolen property was made by his business partners and was related to the walkie-talkies. He stated that he turned himself in to the police; that he remained in jail for a few hours;

---

[7]There is no evidence in the record which supports this statement.

[8]GE 10; GE 11.

[9]GE 10; GE 12; GE 14.

[10]GE 2.

that he talked to his business partners; and that his business partners agreed to drop the charges if he turned over his share of the business to them and would not sue them. He denied any knowledge of a bond being requested for him on these charges and of being charged with felony crimes. He thought these crimes were misdemeanors.[11]

In June 2002, he accepted a position as the Director of Engineering with a company many miles from his residence. In its offer letter, the company agreed to pay him a salary of $70,000 a year, plus benefits. The offer letter noted that the State where he would work was an employment-at-will State and that the letter did not constitute an employment contract. The company asked him to sign a non-competition and non-disclosure agreement, which he signed on June 27, 2010. The company agreed to pay $10,000 for his moving expenses, conditioned upon his working for the company for two years. The offer letter does not discuss the procedure for him to resign. After he moved, Applicant received a bill from the movers for over $20,000. The company agreed to pay the additional moving expenses, if Applicant agreed to remain in the company's employment for three years.[12]

Applicant began his employment in July 2002. His job required him to design and build communication towers and shelters, not to write software. His work involved contracts with the Department of Defense and the State. After his arrival, the company hired his wife as the shop manager and his oldest son as an information technologist (IT). Although Applicant testified that this was part of his hiring contract, the offer letter does not include an offer of employment for his wife and son. The company extended an offer of employment to Applicant's family members after he began work.[13]

For his first year of employment, Applicant performed his work duties on his personal laptop and transferred the information to the company's main server for access by other employees. Even though he received a company laptop computer late in the summer of 2003, he continued performing most of his work on his personal computer and transferring the work to the company server. To do his work, Applicant used software containing a licensing key, which is an electronic code needed to enter the control portion of the system and allow the software to operate. The licensing key has no monetary value or security classification. The licensing key needed to be installed on all equipment related to radios and for repairs. It was on his personal computer, but not his company computer.[14]

The company was delighted with Applicant's work during the first year of his employment. The working relationship between Applicant and the company began to deteriorate in the summer of 2003. The company laid off his wife in 2003, because it

---

[11] *Id*.; Tr. 52-58, 77-81.

[12] GE 3; GE 4; GE 5; Tr. 40.

[13] Tr. 40-41, 48, 59-60, 86-90.

[14] *Id*. at 40-42, 46, 63-64, 72-73, 86-87, 101, 107-110.

was not satisfied with her work, and it reduced the working hours of his son, as it did not need a full-time IT person. Applicant believed the company had financial problems because it laid off other staff, and he was concerned that the company would fail. The company acknowledged that it had some financial problems in the fall of 2003. He believed the company had problems paying vendors, but the company denied this assertion of Applicant. Applicant found other work and asked the company about working part time or moonlighting. The company declined, stating that it needed him to work full time. On November 25, 2003, Applicant sent the company an e-mail, advising that he was resigning his position immediately for reasons already known to the company. He left his locked company laptop, company cell phone with charger, keys, credit card, gas card, and cold weather gear in his locked office. He also advised the company he would contact them soon about "taking care of the relocation issue." Applicant moved from the state by mid-December.[15]

Applicant's sudden departure created problems for the company. In particular, the company discovered that Applicant had erased the system design and the programming for its radio equipment, but not all information on their computer server. Applicant erased work-in-progress and select information from various locations on the network. As a result, the company had to recreate all internal radio programs and designs. On December 1, 2003, the company's attorney wrote a letter to Applicant asking 1) if he was in possession of a DoD system key and programming templates for certain radio programs he designed and related records; and 2) if he had proprietary software which he used to build his designs. The letter also indicated that he had possession of a satellite phone, a specific scanner, 10 company shirts, and two jackets, and that if he did not return this equipment and clothing, the company would bill him for the costs. The company requested reimbursement for his moving costs and payment of outstanding invoices for equipment he had purchased and restoration of the work he had deleted. The company acknowledged that he did not use the key system after he left his employment, and the record contains no evidence that the company's proprietary information was provided to another person or company.[16]

Applicant and the company agreed that he returned the items requested. However, in March 2004, the company filed a lawsuit against Applicant, alleging breach of contract, breach of the covenant of good faith and fair dealing, conversion of tangible personal property, and conversion of certain confidential proprietary personal property. The company sought damages of $86,000, which included the previously paid moving expenses. The court papers were served on a resident of Applicant's new home in May 2004, although Applicant lived and worked overseas at this time. In September 2004, Applicant prepared and mailed a motion for continuance under the Service Member Relief Act, 50 U.S.C. App. 521, Sections 201 and 514, as he was serving overseas in a war zone. At the same time, counsel for the company filed a motion for a default

[15]*Id.* at 43-44, 89-90, 94.

[16]GE 7.

judgment because Applicant had not filed an answer to the lawsuit. The court entered a default judgment on October 6, 2004.[17]

Shortly thereafter, Applicant hired an attorney, who entered an appearance in the lawsuit on October 15, 2004. Upon motion of Applicant's counsel, the court set aside the default judgment on November 24, 2004. Through counsel, Applicant submitted an answer to the civil complaint, wherein he denied the majority of claims and allegations of the company and raised three affirmative defenses to the lawsuit. He also filed a counterclaim against the company for unpaid wages and defamation for wrongful accusations of theft of property. Over the next year, the lawsuit proceeded slowly with motions and trial continuances.[18]

At some point, Applicant advised his counsel that he would be available for the trial in January 2006. The court scheduled the trial for January 17, 2006. Applicant did not appear for the trial, but was represented by his counsel. The court entered its decision on January 20, 2006. After hearing testimony and reviewing the evidence, the court found that Applicant violated the employment agreement, and the company was entitled to recover his moving expenses in the amount of $20,772. The court also found that the information lost in the company's main computer system occurred because Applicant deleted the information and awarded the company $9,035 in damages. The court entered judgment in the amount of $29,807 plus prejudgment interest of $5,532, court costs of $420, and attorney fees of $5,481 in favor of the company and against Applicant. The court decision does not contain any findings on Applicant's counterclaim. Applicant paid the judgment in full in November 2008.[19]

At his security clearance hearing, Applicant explained his conduct in a manner similar to the defenses raised in the lawsuit filed against him by the company. He did not acknowledge deleting any information from the company's computer system. Rather, he indicated the licensing key was on all of the company's computers, meaning access was available to the company.

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.

[17]GE 8; GE 9; AE D.

[18]GE 8; GE 9.

[19]*Id*.

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.

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. . . ." An 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 an applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to 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 E: Personal Conduct

AG ¶ 15 expresses the security concern pertaining to 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.

AG ¶ 16 describes the disqualifying conditions that could raise security concerns. I have considered all the conditions, and especially the following:

(a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(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;

(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 indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of:

(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:

(2) disruptive, violent, or other inappropriate behavior in the workplace;

(3) a pattern of dishonesty or rule violations; and,

(4) evidence of significant misuse of Government or other employer's time or resources;

(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, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group; and

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

During his employment with the company, Applicant worked primarily on his personal computer. He routinely transferred his work product from his personal computer to the company's main computer server, making the work accessible to other employees. When Applicant resigned from the company in 2003, he left the company computer in his company office. He, however, took his personal computer with him which contained company proprietary information. He erased the proprietary information related to the work he performed and transferred to the company's computer server from the company server, causing harm to the company. The company filed a lawsuit against him and the court entered a judgment against him for the harm caused. The police arrested him 1986 and charged him with several misdemeanor and felony crimes. The Government established its case for allegations 1.b, 1.c, and 1.d under AG ¶¶ 16(c), 16(d), 16(e) and 16(f). Because Applicant left the company computer in his office the day he resigned and the offer letter does not provide any requirements for resigning, SOR allegation 1.a is found in favor of Applicant.

For AG ¶ 16(a) to apply, Applicant's omission, concealment or falsification of relevant facts on his e-QIP must be deliberate. The Government established that Applicant omitted a material fact from his SF-86 when he answered "no" to Question 23a, about his criminal felony charges in 1986. This information is material to the evaluation of Applicant's trustworthiness to hold a security clearance and to his honesty. In his response, he denies, however, that he had an intent to hide this information from the Government.

When a falsification allegation is controverted, the Government has the burden of proving it. Proof of an omission, standing alone, does not establish or prove an applicant's intent or state of mind when the omission occurred. *See* ISCR Case No. 07–00196 (App. Bd. Feb. 20, 2009); ISCR Case No. 09-07551 (App. Bd. Mar. 1, 2011) In evaluating whether the Government has presented substantial evidence regarding the deliberate nature of a false statement or an omission, the Judge must examine the statement or omission in light of the record as a whole. *Id*. In making this determination, the administrative judge must determine whether there is direct or circumstantial evidence concerning an applicant's intent or state of mind at the time the omission occurred.

In his response to the SOR, Applicant admitted that he knew this information when he completed the SF 86 and that he sought to conceal the information about his arrest in 1986. He explained at the hearing and in his second interview with the OPM

investigator that he thought the charges were for misdemeanor crimes and had thought so for 25 years. These statements are contrary to his initial statement to the OPM investigator that he thought he need only list crimes for which he served time. His inconsistent statements explaining his answer negatively impact the reliability of his explanation for his "no" answer to Question 23a in the SF 86. The Government has established intentional falsification.

AG ¶ 17 provides conditions that could mitigate security concerns:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;
>
> (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;
>
> (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;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;
>
> (f) the information was unsubstantiated or from a source of questionable reliability; and
>
> (g) association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

Because the factual statement contained in SOR allegation 1.c relates to the conduct raised in SOR allegation 1.b, allegation 1.c is found in favor of Applicant. Allegation 1.d concerns criminal charges which the State decided not to pursue after examining all the evidence. Given the decision of the State, this allegation is found in favor of Applicant. He, however, has not mitigated the security concerns raised in allegations 1.b and 1.e.

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 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 ¶ 40 describes the disqualifying conditions that could raise security concerns. I have considered all the conditions, and especially the following:

> (b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system; and
>
> (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.

When he resigned his position with the company, Applicant decided to erase much of his work product from the company's main computer system. The information deleted from the company's main computer system was not haphazard or all information, but selectively chosen information and primarily related to Applicant's work for the company. Applicant's actions are a violation of the company's policies and general workplace rules governing work products which are the proprietary information of the company. The Government has established a *prima facie* case under Guideline M.

AG ¶ 41 provides conditions that could mitigate security concerns:

> (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.

Applicant's decision to erase information from the company's main computer system was deliberate and intentional, not inadvertent or unintentional. His actions were not for the company's efficiency or effectiveness, but appear to be the result of his anger and frustration with the company. While this incident took place more than seven years ago, given his computer skills and expertise, I have concerns that he could act in a similar manner in the future if he were angry and frustrated with an employer. He has not mitigated the security concerns raised by the Government.

Guideline K: Handling Protection 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 the disqualifying conditions that could raise security concerns. I have considered all the conditions, and especially the following:

(g) any failure to comply with rules for the protection of classified or other sensitive information.

When he resigned his position in 2003, Applicant modified the company's main computer system by erasing much of his work product from the company's main computer system. The information deleted from the company's main computer system was not haphazard or all information, but selectively chosen information and related to Applicant's work for the company. Applicant's actions are a violation of the company's policies and general workplace rules governing work products which are the proprietary information of the company. The Government has established a *prima facie* case under Guideline K.

AG ¶ 35 provides conditions that could mitigate security concerns:

(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's current reliability, trustworthiness, or good judgment;

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and

(c) the security violations were due to improper or inadequate training.

While it has been seven years since Applicant deleted the company's proprietary information connected to his work product, his decision to do so continues to raise concerns that he could act in a similar manner in the future, if he is angry or frustrated with an employer. I recognize that he has handled classified information in the past without incident and since he left the employ of the company in 2003. This positive conduct is insufficient to overcome the concerns I have. He has not mitigated the Government's security concerns under Guideline K.

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 an 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. The decision to grant or deny a security clearance requires a careful weighing of all relevant factors, both favorable and unfavorable. In so doing, an administrative judge must review all the evidence of record, not a single item in isolation, to determine if a security concern is established and then whether it is mitigated. A determination of an applicant's eligibility for a security clearance should not be made as punishment for specific past conduct, but on a reasonable and careful evaluation of all the evidence of record to decide if a nexus exists between established facts and a legitimate security concern.

In reaching a conclusion, I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. After his arrest in 1986, Applicant stayed away from conduct which involved criminal matters. He successfully served in the United States military for seven years, then developed a successful career in communications. His employer highly respects his work skills and rates his performance highly. During his civilian service near the Iraq war zone, he received several awards and letters for his work. The military also thought highly of his work. He has never violated the procedures for handling classified information.

Seven years ago, Applicant abruptly ended his employment with the company after their working relationship deteriorated. When he left his job, he deliberately accessed the company's main computer server and deleted proprietary information related to the work he had performed. This conduct was a serious breach of his responsibilities as an employee and appears to have been done in anger and frustration. He clearly did not want his employer to have access to his work. This conduct raises serious concerns about his judgment and trustworthiness. A concern continues as to what he might do in a similar situation in the future, especially since he has not taken responsibility for his conduct.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the security concerns arising from his misuse of information technoloy and handling of protected information under Guidelines M and K and his personal conduct under Guideline E.

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:	AGAINST APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	For Applicant
Subparagraph 1.d:	For Applicant
Subparagraph 1.e:	Against Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline K:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant

Conclusion

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 Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

MARY E. HENRY
Administrative Judge