



**DEPARTMENT OF DEFENSE  
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:	)	
	)	
SSN:	)	ISCR Case No. 05-02395
	)	
Applicant for Security Clearance	)	

**Appearances**

For Government: Eric Borgstrom, Esq., Department Counsel  
For Applicant: Leslie McAdoo, Esquire

April 30, 2008

**Decision**

---

TUIDER, Robert J., Administrative Judge:

Applicant has not mitigated security concerns pertaining to Misuse of Information Technology, Personal Conduct, and Criminal Conduct. Clearance is denied.

**Statement of the Case**

Applicant submitted his Security Clearance Application (SF 86), on February 21, 2003. On August 1, 2006, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the security concerns under Guidelines M, E, and J for Applicant. The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended and modified (Directive).

Applicant acknowledged receipt of the SOR on August 8, 2006. He answered the SOR in writing through counsel on August 28, 2006, and requested a hearing before an Administrative Judge. DOHA received the request on August 30, 2006. Department

Counsel was prepared to proceed on February 12, 2007, and I received the case assignment on February 13, 2007. DOHA issued a notice of hearing on March 30, 2007, scheduling the case to be heard on May 9, 2007. The hearing was held as scheduled.

The government offered Government Exhibits (GE) 1 through 26, which were received without objection with the exception of GE 19. Counsel for Applicant objected to GE 19 on the basis of authenticity. After argument by counsel, I overruled Counsel for Applicant's objection. Also, because GE 20 consisted of two different parts, it was marked GE 20(a) and 20(b) for clarification purposes. Tr. 18-24, 142-144. Applicant testified on his own behalf and offered Applicant Exhibits (AE) A through Z, without objection. DOHA received the transcript of the hearing (Tr.) on May 25, 2007.

Before the hearing adjourned I held the record open to allow both counsel an opportunity to submit written closing arguments. Department Counsel's closing argument is marked Exhibit (Ex.) I, and Counsel for Applicant's closing argument is marked Ex. II. The record closed on June 14, 2007. Based upon a review of the case file, pleadings, exhibits, and testimony, eligibility for access to classified information is denied.

## **Procedural Rulings**

### **Motion to Amend SOR**

Department Counsel moved to amend the SOR by withdrawing ¶ 2.d., which alleged Applicant was investigated by Naval Criminal Investigative Service (NCIS) concerning several files deleted from his employer's common access drive and cutting tools found to be missing after his employment terminated in March 2001. Without objection from Counsel for Applicant, I granted Department Counsel's motion to withdraw ¶ 2.d., Tr. 239-242.

## **Findings of Fact**

In his Answer to the SOR, dated August 28, 2006, Applicant denied all factual allegations alleged in the SOR. After a thorough review of the pleadings, exhibits, and testimony I make the following findings of fact:

Applicant is a 53-year-old Advisory Engineer, who has been employed by his defense contractor employer since March 2002. He seeks to renew his security clearance and currently holds a secret security clearance, which was initially granted in July 1991. GE 1, Tr. 158-159.

Applicant was born, raised and educated in India. He received his undergraduate education in India and was awarded a Bachelor of Science degree, majoring in Mechanical Engineering, in May 1975. He attended graduate school in the U.S. and received his Master's Degree in Mechanical Engineering, in August 1981. He completed his graduate work in India and was awarded his Ph.D. in Metallurgical Engineering, in

February 1982. GE 5, Tr. 26-27, 160-161. English is Applicant's second language. At home, Applicant speaks a mix of English and "local Indian language." Tr. 162.

Applicant was married in August 1979. He and his wife have two adult children, a daughter and a son, both in their mid-twenties. GE 1, Tr. 157-158.

Applicant was employed at a major state university (university) from March 1, 1984 until he was involuntarily terminated on March 21, 2001. During the 17 years Applicant was employed at the university, he held three different titles, Head of Surface Technologies Department, Professor of Engineering Science and Mechanics, and Senior Scientist. Tr. 26-27, 162-163, GE 7. Evidence submitted by Applicant supports the notion that he was viewed as a valued employee for the vast majority of his university employment. AE F through O. Some time before he was terminated, his relationship with his superior deteriorated, which led to his being involuntarily terminated for "insubordination."<sup>1</sup> GE 7.

On March 21, 2001, Applicant was summoned to a meeting with university officials. When he arrived at the meeting, he was informed he could resign with a severance package, or be involuntarily terminated. He refused to resign and was involuntarily terminated. Tr. 28-30. After working hours that same day, Applicant returned to his work site to collect his personal belongings and clean out his office.

What occurred when Applicant returned to his office is a topic of dispute. Shortly after Applicant left the university, university officials notified NCIS of the improper deletion of numerous sensitive, but unclassified, U.S. Navy and U.S. Marine Corps research files and folders on a shared network drive. Applicant was believed responsible for the improper deletion of the computer files, which occurred on the date of Applicant's termination on March 21, 2001. NCIS conducted an investigation, which is documented in various government exhibits. GE 22 through 26.

The SOR referred to three interviews<sup>2</sup>. Salient portions of those interviews are quoted verbatim in order of chronology<sup>3</sup>:

---

<sup>1</sup> Department Counsel and Counsel for Applicant dedicated portions of their written closing arguments to discussing the underlying basis for Applicant's termination from state university. Ex. I, pgs. 1-4; Ex. II, pgs. 10-14. Regardless of what label is applied as the reason Applicant left university, the fact remains that he was involuntarily terminated on March 21, 2001. Furthermore, he unsuccessfully challenged his termination seeking relief from state/federal administrative/judicial bodies. Applicant's most recent unsuccessful challenge occurred when the Circuit Court of Appeals ruled against him by their Decision on June 30, 2004. GE 11. See also GE 7 through 11, which contain administrative and judicial decisions pertaining to Applicant's unsuccessful challenges to his termination.

<sup>2</sup> I find that all Applicant interviews referred to in this Decision were prepared consistent with existing DoD policy and were provided freely and voluntarily. Tr. 147. See also testimony of DSS Special Agent, who administered Applicant's two October 2005 signed, sworn statements. Tr. 175-195

<sup>3</sup> Quoting the Applicant/source documents was chosen versus summarization to accurately reflect what was, in fact, said. It also demonstrates the contrast in Applicant's statements. Also, See Applicant's testimony. Tr. 25-168.

**August 9, 2001 NCIS Interview.**<sup>4</sup>

[Applicant] advised that after receiving this news (being involuntarily terminated) he walked around the campus for a short period and eventually returned to his office [at university]. [Applicant] reported that when he returned to his office he didn't touch anything and telephoned his wife. Following the telephone call he claimed that he left the office at approximately 5:10-15pm and went to get his wife to tell her about the firing. [Applicant] claimed that he and his wife went directly home and that he did not return to the campus until 6:45-7:00 pm. [Applicant] said that when he returned to the campus he merely wanted to collect his many personal belongings and clean out his office. [Applicant] reported that he took plastic garbage bags from home to use when he threw away personal items only. [Applicant] said he didn't see anyone upon his return aside from one new employee. [Applicant] advised that he then removed his books, thesis papers, etc., and took them to his car and threw away magazines and other periodicals. He also claimed that he deleted personal e-mails from the computer network. **According to [Applicant], he also deleted his personal papers, thoughts and ideas from the computer in his office. [Applicant] adamantly denied destroying non-personal research data, tool specimens or other Government program material.** [Applicant] confirmed that a "bios" password existed on the local machines hard drive and stated he felt confident that no one, other than he, could gain access to the data on his work computer. [Applicant] concluded by stating that his computer was on when he left to attend the meeting with [university officials] and that he didn't touch it again until after he returned from home at approximately 6:45-7:00 pm.

Following the above interview, [Applicant's attorney] was provided with an Excel spreadsheet that shows a significant amount of files, to include program related items, files and folders, being deleted on March 21, 2001 from approximately 3:18 pm through 10:09 pm. [Applicant's attorney] asked reporting agent if he could consult further with his client prior to answering specific questions relating to file deletions. [Applicant's attorney] also stated that his client would be available in the future to answer additional questions regarding this matter after reviewing the deleted file list. GE 23, pgs. 4-5. (SOR ¶ 2.c.)

---

<sup>4</sup> This interview was conducted in the presence of Applicant's attorney and was prepared by the reporting agent as a summarized result of interview.

**October 20, 2005 Interview.**<sup>5</sup>

**I did not delete or destroy computerized record (sic) from [a university] computer that contained US Navy proprietary information that dealt with aircraft engine parts and components. I did not delete files from the [university] shared network.** I have been told by [DSS Special Agent] that NCIS agents said I was accused of deleting or destroying over 3500 files at [university] after my termination. **I deny this.** GE 5, pg. 2.

**January 26 2006 Interview.**<sup>6</sup>

On the day that I was fired, I was called to meet with [university's] Human Resources Manager (HRM). I was told the reason for the meeting was to discuss some issues that I had raised such as my complaint of discrimination, credit due for my patents, etc. When I went to [HRM's] office, [Second Level Supervisor(SLS)] was also in my office. I must say that I was surprised to see [SLS] in the office. He was my second level supervisor. I was asked to resign my position at [university]. I was told that if I did not resign, then I would be fired immediately. I chose not to resign, so I was told that I was fired. I understood that I was fired within seconds and I asked [HRM] for the letter notifying me that I was fired and the reason(s) for my termination. I was told that there was no letter, but I could return on another day for written notice of my termination. I indicated that I would return the following day. After leaving [HRM's] office, I picked up my wife from her workplace. I told her that I had just been fired from my job and it was like she was in shock. She didn't say a word. We drove home and talked some more about what had happened to me. I told her that I planned to visit with [university officials] the following day. I did not feel what they did to me was right. I received no warning and I was deceived about the true reason of my meeting with [HRM].

The more I thought about what had happened, I came to the decision to go back to my office that evening in order to gather my personal belongings. I went at night because I felt it might be difficult for me to face my colleagues the following day. I estimate that I arrived at my office at approximately 6:00 PM that same day that I was terminated. I remained at my office for about 90 minutes, which meant that I left at about 7:30 PM. While in my office, I gathered my belongings. I found some boxes and some garbage bags for trash and/or my personal effects. Some of the

---

<sup>5</sup> This Applicant interview is a signed, sworn, statement conducted by a Special Agent of the Defense Security Service (DSS).

<sup>6</sup> This Applicant interview is a signed, sworn statement that was taken before a scheduled DSS polygraph. In light of Applicant's admissions, the polygraph phase of the examination was not conducted. GE 3, GE 4.

items that I collected were numerous professional books. Some of these books belonged to me and some belonged to [university libraries]. My intention for gathering the library books was so that I could return them to the respective library. I estimate that there were approximately 10 to 15 library books in total. I did in fact return all of these books to their respective library. Earlier today, I told [DSS Special Agent] that I did in fact delete most or all of my email from my [university] office computer that night. I felt that no one needed access to my email. I also searched for and deleted numerous files that I had created and stored on my local computer drive. I explained that these files although professional in nature, were my thoughts, ideas, etc and were not any of the estimated 3500 missing files in question that were stored on the common access drive. (The files that contained US Navy/DoD related information.) I stated that with some of these smaller documents, I printed some of them for my future use. I explained to [DSS Special Agent] that as a professor, I needed to be on the cutting edge. I also stated that I did not want anyone else to have access to my ideas and thoughts. I also acknowledged to [DSS Special Agent] earlier today that it was very possible that I had deleted some files located on the common access drive, but it was done accidentally. In other words, I was in a hurry. I had also told [DSS Special Agent] that although I am a scientist, I am not as knowledgeable about computers as other people are. I told [DSS Special Agent] earlier today that I did not delete any files out of anger or revenge. I also explained that some files not found on the common access drive might have also been ones on my local drive that were deleted.

[DSS Special Agent] provided me with a break to obtain something to eat. Upon my return, he began to review with me the polygraph examination questions. The first question that he read was "Did you delete any of those [university] common access computer files on purpose that night?" I answered "Yes". In talking with [DSS Special Agent] further about this matter, **I admitted that I did in fact deliberately delete many files that were stored on the [university] common access drive.** I have been told several times that it was reported that approximately 3500 or more files were deleted from the [university] common access drive during the evening hours on the day I was terminated. These files reportedly contained US Navy/DoD related information. [DSS Special Agent] informed me today that one estimate indicated that the deletion or damage of these files caused an approximate loss of \$20,000 to [university]. [DSS Special Agent] has further told me that the US Attorney declined to prosecute me because a majority of the files were recovered. As indicated above, I did in fact delete multiple files from the [university] common access drive. I honestly did not count the number files that I deleted. I don't believe that the number of deleted files was as high as 3500, but I cannot state for sure the number of files that I deleted. **Nonetheless, I now admit that the many of the missing files in question were files**

**that I deleted on the [university] common access drive. At the time that I deleted these files that were stored on the [state university] common access drive, I felt that it was my information that I had developed and no one else had a right to access it.** I did not believe that the information belonged to [university] or the US Navy. I acknowledge that the [university] and the US Navy had a different opinion about the deleted files and they believed that it was proprietary information that belonged to the USN / [university]. Although I did not believe it at the time, I can now understand how they could think that they had rights to the information contained in the files that I deleted. I want to further state that I now have no qualms about the US Navy / [university's] opinion that the information belonged to them. After all, I used their computer(s), their facilities, etc. I told [DSS Special Agent] that if I could do it all over again, I would not have deleted those files. I want to go on record and state that I would never do something like this again in the future. Also, while at lunch today, I thought about a situation with my daughter that occurred several years ago. She told me that I was stubborn. The more I thought about this today, I began to think that perhaps this could apply to this situation with the [university] missing computer files. Earlier today, I told [DSS Special Agent] that I did not delete any files out of anger or hostility for being fired, but I admit that perhaps that is not realistic. Perhaps out of my "stubbornness", I have been in a denial mode that I was angry at the time of my termination, but maybe was truly angry. At the very least, as indicated above, I did not want people to have access to the information that I had worked on over the years.

I acknowledge that [DSS Special Agent(1)<sup>7</sup>] interviewed me on 20 and 26 October 05 as part of my DoD security clearance investigation. When [DSS Special Agent] called me, she gave me a general idea of what we would be talking about. I provided a brief explanation to her over the phone and she asked me to prepare an explanation in writing and bring it to our interview. I did in fact prepare written responses and these are incorporated into my sworn written statement, dated 20 Oct 05. In that sworn written statement, it reflects on page two of five that I did not delete or destroy computerized records from [university] computer that contained US Navy proprietary information that dealt with aircraft engine parts and components. I further indicated that I did not delete files from the [university] shared network. I indicated that [DSS Special Agent] informed me that I was suspected or accused of deleting or destroying an estimated 3500 files at [university] and I denied this allegation. On page four of five, I indicated that although I deleted my personal emails, I did not delete any files related to my work. I explained that I had an informal meeting with the

---

<sup>7</sup> The DSS Special Agent, who took Applicant's signed, sworn statement on October 20 and 26, 2005 was a different Agent than the Agent who took Applicant's January 26, 2006 signed, sworn statement.

NCIS in my attorney's office and I had reiterated that I did not delete any files related to my work.

[DSS Special Agent] pointed out to me that there is a large difference between what I told [DSS Special Agent(1)] and what I told him today. In trying to explain the differences in my statements, I told him that there was no intent to lie to [DSS Special Agent(1)] or deliberately omit critical information. I explained to [DSS Special Agent] that at the time of my interview with [DSS Special Agent(1)], I still did not believe that the files I deleted were proprietary information belonging to the US Navy or [university]. Even though my previous statement clearly reads that I only deleted email and I did not delete any files related to my work, I did not think of the fact that I did delete various professional files from the common access drive. I understand that persons reading my statements might come to the conclusion that I was not honest with [DSS Special Agent(1)], but I did not lie to her or provide a false statement. Listening to [DSS Special Agent] today, it helped me to re-think what happened and to think about perceptions versus reality. My perception was different from the US Navy or [university's] perception of what happened. GE 2, pgs. 2-5 (emphasis added).

On the evening Applicant deleted files from the common access drive, he printed documents for his future use and acknowledged he "may have printed something less than five, small documents." Tr. 37-38. (SOR ¶ 1.b.)

When Applicant was hired by the university, he executed a Loyalty Oath. GE 20(a). At his hearing, he acknowledged that any intellectual property he created during the course of his employment with the university belonged to the university. Tr. 118-119. He executed an Agreement Concerning Proprietary Rights with the university on March 2, 1984, which elaborated on this notion. GE 20(b). The university also has established policy restrictions on the use of the university computer system and sanctions for failing to comply with university policies. Tr. 138-141. See university computer and network security policy document, GE 21.

At his hearing, Applicant deviated from his admission in the January 2006 Interview. In an effort to capture the essence of Applicant's position, I summarized his position with him at his hearing. Applicant testified he only deleted his personal e-mails from his university computer account, i.e. if it had a "From" or "To" line, he considered the e-mail to be personal and if an e-mail had an attachment, it was "eliminated automatically." Applicant now understands personal to mean e-mails which would include such things as an e-mail to his wife or his children or planning for a picnic. He added that "anything research-related" or "project-related" was non-personal. "But that was not my understanding when I was deleting those files. I thought this was all my personal communication. And it is a broader meaning of the word personal that I had on my mind." Tr. 166-167. See *a/so* Applicant's testimony, Tr. 25-167; Department



Counsel's closing argument (Ex. I), pgs. 16-26; and Counsel for Applicant's closing argument (Ex. II), pgs. 16-31.

## **Policies**

When evaluating an Applicant's suitability for a security clearance, the Administrative Judge must consider the 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. The Administrative Judge's over-arching adjudicative goal is a fair, impartial and common sense decision. The entire process includes 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 ¶ E2.2.2. requires that "[a]ny doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the Applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The Applicant has the ultimate burden of persuasion as to 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 the 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 M, Misuse of Information Technology Systems**

The security concern relating to the guideline for Misuse of Information Technology Systems is set out in AG ¶ E2.A13.1.1.:

Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual’s trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

The applicable guideline lists four Disqualifying Conditions that could raise security concerns. Under AG ¶ E2.A13.1.2.:

AG E2.A13.1.2.1. (IT DC 1): Illegal or unauthorized entry into any information technology system;

AG E2.A13.1.2.2. (IT DC 2): Illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system;

AG E2.A13.1.2.3. (IT DC 3): Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations; and

AG E2.A13.1.2.4. (IT DC 4): Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

AG E2.A13.1.3. lists four Mitigating Conditions under this concern:

AG E2.A13.1.3.1. (IT MC 1): The misuse was not recent or significant;

AG E2.A13.1.3.2. (IT MC 2): The conduct was unintentional or inadvertent;

AG E2.A13.1.3.3. (IT MC 3): The introduction or removal of media was authorized;

AG 32.A13.1.3.4. (IT MC 4): The misuse was an isolated event; and

AG E2.A13.1.3.5. (IT MC 5): The misuse was followed by a prompt, good faith effort to correct the situation.

Having carefully reviewed the evidence, I conclude Applicant intentionally deleted U.S. Navy proprietary files, containing unclassified, but military critical information, from a shared database from his employer's computer without permission after he was involuntarily terminated from university on March 21, 2001. (SOR ¶ 1.a.) Having made this finding, application of IT DC 3 cited *supra* is the most pertinent Disqualifying Condition. I do not accept Applicant's explanations, particularly those offered at his hearing. Weighing heavily against him were his admissions contained in his January 26, 2006 pre-polygraph statement to DSS. GE 2. See Guideline E discussion *infra*.

Insufficient evidence was developed regarding the nature and quality of the approximate five documents Applicant printed following his involuntary termination on March 21, 2001. (SOR ¶ 1.b.) Viewing the facts in the light most favorable to the Applicant, I find application of any Disqualifying Conditions to SOR ¶ 1.b. unwarranted.

### **Guideline E, Personal Conduct**

The security concern relating to the guideline for Personal Conduct is set out in AG ¶ E2.A5.1.1.:

Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

AG E2.A5.1.1.1. Refusal to undergo or cooperate with required security processing, including medical and psychological testing; or

E2.A5.1.1.2. Refusal to complete required security forms, releases, or provide full, frank and truthful answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

The applicable guideline lists six Disqualifying Conditions that could raise security concerns under AG ¶ E2.A5.1.2.:

AG E2.A5.1.2.1. (DC PC 1): Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

AG E2.A5.1.2.2. (DC PC 2): The deliberate omission, concealment, or falsification of relevant and material 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;

AG E2.A5.1.2.3. (DC PC 3): Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;

AG E2.A5.1.2.4. (DC PC 4): Personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or duress, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail;

AG E2.A5.1.2.5. (DC PC 5): A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency; and

AG E2.A5.1.2.6. (DC PC 6): Association with persons involved in criminal activity.

AG E2.A5.1.3. lists seven Mitigating Conditions under this concern:

AG E2.A5.1.3.1. (MC PC 1): The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

AG E2.A5.1.3.2. (MC PC 2): The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

AG E2.A5.1.3.3. (MC PC 3): The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

AG E2.A5.1.3.4. (MC PC 4): Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

AG E2.A5.1.3.5. (MC PC 5): The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;

AG E2.A5.1.3.6. (MC PC 6): A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information; and

AG E2.A5.1.3.7. (MC PC 7): Association with persons involved in criminal activities has ceased.

Applicant's involuntary termination from university on March 21, 2001 was clearly established by the evidence. (SOR ¶ 2.a) Both counsel dedicated portions of their written closing arguments discussing the characterization of Applicant's termination. Regardless of how one chooses to characterize his termination, the fact remains Applicant was involuntarily terminated and all of his subsequent administrative and judicial appeals were unsuccessful. These facts warrant application of DC PC 1 as a Disqualifying Condition. However, having concluded DC PC 1 is applicable, I cannot ignore the fact Applicant had a very successful 16-year career with university until he was involuntarily terminated, and also has had a seven-year successful career with his subsequent employer. I do not view Applicant's difficulties with university as systemic or ongoing. While none of the Mitigating Conditions under this concern appear particularly on point, mitigation is available to Applicant under the "Whole Person" discussed *infra*.

The Government withdrew SOR ¶ 2.b. Accordingly, further discussion regarding this allegation is not warranted.

This brings the discussion to the gravamen of this case, i.e. Applicant's honesty and credibility which are brought into question by SOR ¶¶ 2.c. through 2.e. As alleged, Applicant initially denied deleting numerous files containing proprietary information in his August 9, 2001 and October 20, 2005 interviews, and initially at his pre-polygraph January 26, 2006 interview. With the exception of his August 9, 2001 interview, which is summarized, the remaining October 20, 2006 and January 26, 2006 interviews are signed, sworn statements. The interviews/statements cited verbatim *supra* with emphasis added clearly demonstrate a significant disparity from what Applicant was initially reporting to Government investigators versus what he reported in his January 26, 2006 interview.

In evaluating which explanation deserves greater weight, I reviewed each statement under the context in which it was provided. The August 9, 2001 interview was conducted approximately five months after Applicant was involuntarily terminated from university, and Applicant's counsel was present during this interview. In Applicant's October 20, 2005 interview, he again reiterated his earlier denial. Almost five years after being involuntarily terminated and in conjunction with the renewal of his security clearance, Applicant was interviewed on January 26, 2006. On this day, Applicant was scheduled to take a polygraph examination and before administering the examination, the DSS Special Agent/Polygrapher interviewed Applicant. This interview resulted in

Applicant conceding that he deliberately deleted proprietary information on the day he was involuntarily terminated. Applicant's admissions were reduced to writing and were incriminating. See Applicant's verbatim statements under Findings of Fact *supra*.

What appears more plausible is Applicant's January 26, 2006 version of what happened. Understandably, Applicant was distraught and angry after being involuntarily terminated from a job he had successfully held for 17 years. Without belaboring the underlying reasons Applicant provided surrounding his termination, he considered the work he deleted to be his and furthermore that no one had a right to access it. The evidence establishes and Applicant concedes the information on the university's common access drive was proprietary information that belonged to the university.

I do not accept Applicant's subsequent statements that whatever he deleted was "personal," "inadvertent," or "unintentional." He was and is an intelligent, well educated person. I also note Applicant spent his working life in the U.S. and was a tenured professor with a Ph.D. in Mechanical Engineering. He conducted his professional life speaking, reading and writing in English and he is credited with numerous publications. It is unfortunate Applicant chose to destroy the proprietary information he did. No doubt, if given the choice to relive March 21, 2001 again, he would choose differently. That choice placed him in a position that required him to later admit or deny his wrongdoing. Again, he made a choice that had repercussions. After reviewing the evidence, application of DC PC 3, DC PC 4, and DC PC 5 appear most appropriate. No Mitigating Conditions under this concern are applicable *supra*.

## **Guideline J, Criminal Conduct**

The security concern relating to the guideline for Criminal Conduct is set out in AG ¶ E2.A10.1.1.:

A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

The applicable guideline lists two Disqualifying Conditions (CC DC) that could raise security concerns under AG ¶ E2.A10.1.2.:

AG E2.A10.1.2.1. (CC DC 1): Allegations or admission of criminal conduct, regardless of whether the person was formally charged; and

AG E2.A10.1.2.2. (CC DC 2): A single serious crime or multiple lesser offenses.

AG E2.A10.1.3. lists six Mitigating Conditions under this concern:

AG E2.A10.1.3.1. (CC MC 1): The criminal behavior was not recent;

AG E2.A10.1.3.2. (CC MC 2): The crime was an isolated incident;

AG E2.A10.1.3.3. (CC MC 3): The person was pressured or coerced into committing the act and those pressures are no longer in that person's life;

AG E2.A10.1.3.4. (CC MC 4): The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;

AG E2.A10.1.3.5. (CC MC 5): Acquittal; and

AG E2.A10.1.3.6. (CC MC 6): There is clear evidence of successful rehabilitation.

By its very nature, this concern calls into question a person's ability or willingness to comply with laws, rules, and regulations. The government established its case under this concern by showing that Applicant falsified his interview(s)/sworn statement(s) as alleged in SOR ¶¶ 2.c., 2.d., and 2.e. I find, as discussed *supra* under Guideline E, that Applicant deliberately falsified these interview(s)/sworn statement(s). His falsifications are material and a violation of 18 USC § 1001, a felony.<sup>8</sup>

Applicant's recent falsifications bring to the forefront the criminal conduct concerns raised by his past behavior. I am required to consider Applicant's overall questionable behavior when evaluating the seriousness of the conduct alleged in the SOR to determine factors such as the extent to which his behavior is recent, the likelihood of recurrence; and Applicant's explanations concerning the circumstances of the incidents alleged.<sup>9</sup>

Under the totality of the circumstances, I find Applicant's criminal behavior is recent and not isolated. Considering his criminal behavior, the nature and seriousness of his misconduct, his falsifications of his interview(s)/sworn statement(s), and his overall conduct as established by the government, I find his favorable information is not sufficient to mitigate the Guideline J security concerns. His behavior raises questions about his ability and willingness to follow the law, and ultimately, to protect classified information. His recent falsifications and lack of candor weigh against a finding of rehabilitation and positive behavioral changes. Accordingly, No Mitigating Conditions under this concern are applicable *supra*.

### **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

---

<sup>8</sup> It is a criminal offense to knowingly make any materially false, fictitious, or fraudulent statement or representation, or knowingly make or use a false writing in any matter within the jurisdiction of the executive branch of the Government of the United States. Security clearances are within the jurisdiction of the executive branch of the Government of the United States. *Egan*, 484 U.S. at 527 (discussing 18 USC § 1001).

<sup>9</sup>ISCR Case No. 04-09959 at 3 (App. Bd. May 19, 2006).

conduct and all the circumstances. The Administrative Judge should consider the nine adjudicative process factors listed at AG ¶ E2.2.1.: “(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 voluntariness of participation; (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 ¶ 2.2.3., the ultimate determination of whether to grant eligibility for a security clearance must be an overall common sense determination based upon careful consideration of the guidelines and the whole person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I note that except for being involuntarily terminated on March 21, 2001, Applicant has enjoyed a very successful professional life. He and his wife raised two children, who are successful and productive members of society. When Applicant’s termination is contrasted with his other lifetime accomplishments, it is relatively small by comparison. His difficulties at university are not ongoing and are isolated. Accordingly, under the “Whole Person Concept,” SOR ¶ 2.a. is deemed mitigated.

Unfortunately, Applicant’s deletions of proprietary information and subsequent falsifications surrounding those deletions are a different matter. The best indicator of future behavior is past behavior. Applicant’s conduct as it pertains to SOR ¶¶ 1.a., 2.c. through 2.e., and 3.a. raises lingering security concerns. His subsequent denials of wrongdoing at his hearing suggest to me that he is unwilling to accept responsibility for his actions and/or was attempting to divert his accountability or was simply not being truthful.

Overall, the record evidence leaves me with questions or doubts as to Applicant’s eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant had not mitigated the security concerns arising from his Misuse of Information Technology Systems, Personal Conduct, and Criminal Conduct considerations.

### **Formal Findings**

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline M:	AGAINST APPLICANT
Subparagraph 1.a.:	Against Applicant
Subparagraph 1.b.:	For Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT



Subparagraph 2.a.:	For Applicant
Subparagraph 2.b.:	Withdrawn
Subparagraph 2.c.:	Against Applicant
Subparagraph 2.d.:	Against Applicant
Subparagraph 2.e.:	Against Applicant
Subparagraph 2.f.:	Against Applicant
Paragraph 3, Guideline J:	AGAINST APPLICANT
Subparagraph 3.a.	Against Applicant

### **Conclusion**

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

---

ROBERT J. TUIDER  
Administrative Judge