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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| [Name Redacted] | ) | ISCR Case No. 15-05523 |
| | ) | |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Rhett Petcher, Esquire, Department Counsel
For Applicant: *Pro se*

04/19/2017

## Decision

HOGAN, Erin C., Administrative Judge:

On April 13, 2016, the Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline K, Handling Protected Information; Guideline M, Use of Information Technology Systems; and Guideline E, Personal Conduct. 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 (AG) implemented within DOD on September 1, 2006.

On April 22, 2016, Applicant answered the SOR and requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). On September 15, 2016, Department Counsel was ready to proceed. On October 28, 2016, the case was assigned to me. On November 10, 2016, a Notice of Hearing was issued, scheduling the hearing on December 8, 2016. The hearing was held on that date. The Government offered five exhibits which were admitted as Government Exhibits (Gov) 1-5. Applicant testified, called two witnesses and offered one exhibit consisting of numerous documents which was marked as Applicant Exhibit (AE) A. DOHA received the transcript on December 16, 2016. The record was held open until December 22,

2016, to allow Applicant to submit additional documents. Applicant timely submitted a document that was admitted as AE B. Based upon a review of the case file, pleadings, exhibits, and testimony, eligibility for access to classified information is granted.

## Findings of Fact

Applicant is a 54-year-old employee of a DOD contractor. He has worked for his current employer since November 4, 2013. He has held a security clearance since 1987. For over 30 years, he has worked for various contractors supporting several government agencies. He has had a security clearance for 30 years. He has a bachelor's and two master's degrees. He is married and has four adult children. (Tr. 133-35; Gov 1) (Some details have been excluded in order to protect Applicant's right to privacy. Specific information is available in the cited exhibits.)

The SOR alleged two allegations under Guideline K. The first allegation was that Applicant violated Contractor A's Non-Disclosure and Invention Assignment Agreement, signed by Applicant in July 2008, when he copied files that contained company confidential and proprietary information from his company computer to his personal removable media drives (i.e. thumb drives) on multiple occasions between June 2011 and April 2012, resulting in the unauthorized copying of 1,700 files. The second allegation involved Applicants' retention of Contractor A's computer files containing company confidential and proprietary information after certifying in April 2012 that he did not have such information in his possession when he signed Contractor A's Termination Certification.

The Guideline K allegations were also cross-alleged Under Guidelines M and E. Under Guideline E, the SOR also alleged that Applicant falsified information during interviews with DOD authorized investigators on June 20, 2013 and August 12, 2014, when he said that he accidentally copied company confidential and proprietary information from his company computer to his personal removable media drives. It is alleged that Applicant's actions were deliberate.

In July 2008, Applicant was hired by Contractor A. On July 14, 2008, Applicant signed a Non-Disclosure and Invention Assignment Agreement. The agreement defines "proprietary information" in great detail. It reads:

> I agree at all times during my employment with the Company and at all times hereafter to hold the strictest confidence and not to use, publish, disclose, transfer, deliver, or divulge any Proprietary Information: (a) for my own benefit and for the benefit of any person, entity, or corporation other than the Company; or (b) to any person who is not a current employee of the Company, except in the performance of the duties assigned to me by the Company, at any time prior or subsequent to the termination of my employment with the Company, without the express written consent of the Company. I further agree not to make electronic or hard copies of any Proprietary Information, except as authorized in writing

> by the Company. I acknowledge that my obligations under section 1 shall survive the termination of my employment with the Company regardless of the reason for the termination. (Gov 4 at 2)

In 2011, Applicant's boss left Contractor A. Applicant believed that he was groomed to take his spot. Contractor A's Chief Executive Officer (CEO) decided that he wanted to look outside the company for a potential hire to take Applicant's boss's position. Applicant thought it unlikely that he would get the position. Because he was passed over for promotion, Applicant did not believe that he had a future at Contractor A. He began to look for another job. In early 2012, he learned the CEO had hired someone from outside the company. (Tr. 38-40, 42; Gov 5 at 4).

On March 28, 2012, Applicant received a job offer from Contractor B. On April 3, 2012, he resigned from Contractor A and accepted the job offer. On April 5, 2012, Applicant signed a Contractor A Termination Certification. The first paragraph of the certification states:

> I hereby certify that I do not have in my possession, nor have I failed to return, any and all memoranda, notes correspondence, databases, discs, records, reports, manuals, books, papers, letters, CD Roms, keys, Internet database access codes, client profile data, orders, customer lists, contracts, software programs, information and records, drafts of instructions, and other documentation (whether in draft or final form), and other sales, financial or technical information relating to the business of [Contractor A] or its subsidiaries, parents, affiliates, successors or assigns (together, the "Company"), and any and all other documents containing Proprietary Information (as defined in the Non-Disclosure and Inventions Assignment Agreement) furnished to me by any representative of the Company or otherwise acquired or developed by me in connection with my association with the Company, including all Third Party Information. (Gov 4 at 9-10)

On the day Applicant signed the Termination Certificate, he had about three more weeks to work at Contractor A. When he was asked to sign the letter, he was in a hurry because he was leaving on vacation. He did not read the termination certificate carefully. (Tr. 34, 54-56)

On April 5, 2012, the same day that Applicant left on vacation, Contractor A's Data Loss Prevention office prepared a report indicating that Applicant had copied from his Contractor A-issued laptop computer to "removable media" approximately 1,470 files, some of which contained Contractor A proprietary information. The file transfers occurred between February 5, 2012 and April 2, 2012. The majority of the files were transferred to removable media on March 9, 2012 (886 files) and March 18, 2012 (408 files). None of the files contained classified information. (Item 5 at 4; *see also* Tr. 36, 41, 43-46)

On April 12, 2012, Applicant returned from vacation. Employees at Contractor A confronted him about his downloading of proprietary information and he was immediately terminated. Contractor A also contacted Contractor B about the files transfer and Contractor B withdrew their job offer. Applicant was unemployed from April 19, 2012 to July 14, 2012. (Tr. 34, 54-60)

During the investigation, Applicant was asked to provide his personal desktop computer and two personal laptop computers to the company for forensic examination. He cooperated with the investigation. Applicant also provided six removable media (i.e. thumb drives), one iPod, and his Contractor A-issued laptop computer for forensic examination. The investigation revealed Applicant transferred files, some of which contained Contractor A proprietary information, to his personal laptop on February 5, 2012 (137 files); February 18, 2012 (34 files), March 9, 2012 (886 files); March 18, 2012 (408 files) and April 2, 2012 (20 files). It is not clear how many of the files contained proprietary information. Applicant transferred several files that contained personal non-proprietary information on February 10, 2012, and February 19, 2012. (Item 5 at 4-5)

Applicant's security clearance was suspended when Contractor A opened an investigation regarding his transfer of proprietary information to his home computer. The Defense Security Service (DSS) was involved in the investigation. According to Applicant, DSS concluded that there was no breach of security and no classified information was compromised. After the investigation, Applicant's security clearance was reinstated. (Gov 2 at 7)

In his response to the SOR, Applicant admits to making two fundamental errors at Contractor A. First, he transferred data that was unclassified and company proprietary from his Contractor A flash drive to his home computer using an improper process. Second, he did not read the Contractor A Termination Certification thoroughly. He deeply regrets making these two errors and states that his actions were not malicious. Applicant states that he has over 28 years of handling proprietary information and classified documents and stands by his record. He believes he can be trusted to handle classified information. As a result of the incident at Contractor A, Applicant suffered a period of unemployment and had to accept a job with a 25% decrease in income. The event significantly heightened his sense of document and security awareness. (Answer to SOR, dated April 21, 2016)

Applicant claims most of the files he transferred were photographs that he wanted to keep from his business travels with Contractor A. During the investigation, he was not provided access to the list of the files, but disputes the number of proprietary files. When confronted by Contractor A in April 2012, he immediately surrendered his home computer to the Facility Security Officer (FSO) and cooperated with the investigation. The proprietary information stored on his home computer's hard drive was not transferred to any other source. He realizes he should have consulted with management before transferring the data. (Id.)

Applicant states that Contractor A requested that he sign the Termination Certificate three weeks before his last day. On the day he signed it, he was leaving for vacation and quickly read and signed it. He planned on completing paper work and clearing out his office when he returned from vacation. He realizes that this is not an acceptable excuse and admits to his error. He is now much more attentive on reading detailed documentation. (Id.)

Applicant says some of the files were transferred when he was teleworking. He admits transferring the files to a home computer was the incorrect process. To save time, he transferred many files of information at one time. He planned to delete the proprietary files later. He states that he should have made a folder of the non-proprietary files and sought company approval before transferring the documents. (Id.)

Applicant denies the falsification allegation in SOR ¶ 3.b, which alleges that he falsified material facts during interviews with DOD investigators on June 20, 2013 and August 12, 2014 when he stated that he accidentally copied company confidential and proprietary information from his company computer to his personal removable media drives. The statement is alleged to be false in that he deliberately copied files containing company confidential and proprietary information from his company computer to personal removable media drives on multiple occasions between June 2011 to April 2012, copying 1,700 files. Applicant claims that his statement to investigator was taken out of context. He explained to the investigator that he did not follow proper procedures when transferring his personal files to his home computer. Applicant is aware that Contractor A tracks the transfer of all files. Applicant says he was honest and cooperated during Contractor A's investigation. (Id.)

Applicant believes he is trustworthy to hold a security clearance. Since this event, he has followed the highest employment standards while working with two subsequent defense contractors. (Contractor C and Contractor D.) He handled both Secret and Top Secret documents without incident during their employment. (Id.)

During the hearing, Applicant said that he was disappointed in himself because he did not follow the proper procedures for protecting proprietary information. When Applicant was leaving the company, he intended to keep unclassified open source documents. He transferred entire files with the intent to keep the open source documents and delete the proprietary information before he left Contractor A. He had no intention to keep the proprietary information. He was aware the information was tracked by Contractor A. (Tr. 25-32)

Applicant transferred the files when he had time. He did not look at the folders when he transferred them. He intended to delete the proprietary information later. He could have separated the proprietary information before transferring the files to his home computer. If he could do it all over again that is how he would transfer the files. When Applicant transferred the files, he was aware that there was proprietary information in the files. It did not enter his mind that he was violating company policy. (Tr. 47-48, 62)

## Whole-person Factors

Applicant worked for Contractor E from May 1997 to July 2008 and previously from June 1987 to May 1997. (Gov 2 at 8) Mr. C., Applicant's supervisor at Contractor E from 1988 to 2004, testified at the hearing. He never recalls Applicant violating security rules or company rules. There was a team security violation in 1999. It was an inadvertent disclosure of classified information. Mr. C. does not remember the details of the violation. (Applicant brought up the issue of this incident during his questioning of the witness. He indicated that he wanted to provide full disclosure.) Mr. C. worked with Applicant on a daily basis. He believes Applicant is trustworthy to have a security clearance. He said that during the time he supervised Applicant, he made significant contributions to the war effort. He is not exactly aware of the specific SOR allegations, but is aware that it involved Applicant taking home proprietary information. Mr. C. advised that proprietary information is different from classified information. (Tr. 69-76)

Mr. P., Applicant's current supervisor from Contractor D, testified on his behalf. He has supervised Applicant since he was hired about three years ago. He works with Applicant on a daily basis. Mr. P. works on classified projects with Applicant. He states that Applicant is conscientious about handling classified information. He does not hesitate to recommend Applicant for a security clearance. Applicant provided a copy of the SOR to Mr. P. He still recommends Applicant for a security clearance. He indicates that Contractor D has regular security training which Applicant attends. (Tr. 78 – 86)

Applicant provided his employee reviews from Contractor A for 2008, 2009, 2010, and 2011. All were favorable. He was selected for and completed Contractor A's Executive Development Program on January 24, 2012. He also provided two Letters of Appreciation from the Chief Executive Officer (CEO) of Contractor A from June 2009 and March 2011. (AE A) After the hearing, Applicant provided his employee reviews from his two subsequent employers, Contractor C and Contractor D. All were favorable. (AE B)

## 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 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, 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 that 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).

The Government's substantial evidence and Applicant's own admissions raise security concerns under Guideline H, Drug Involvement. The burden shifted to Applicant to produce evidence to rebut, explain, extenuate, or mitigate the security concerns. (Directive ¶ E3.1.15) An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. (*See* ISCR Case No. 02-31154 at 5 (App. Bd. September 22, 2005))

**Guideline K, Handling Protected 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 conditions that could raise a security concern and may be disqualifying:

> (a) deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences;
>
> (b) collecting or storing classified or other protected information at home or in any other unauthorized location;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, game board, handheld, "palm" or pocket device or other adjunct equipment;
>
> (d) inappropriate efforts to obtain or view classified or other protected information outside one's need to know;
>
> (e) copying classified or other protected information in a manner designed to conceal or remove classification or other document control markings;
>
> (f) viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information;
>
> (h) negligence or lax security habits that persist despite counseling by management; and,
>
> (i) failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent.

I find that AG ¶¶ 34(b), 34(c), and 34(g) apply to Applicant's case. AG ¶ 34 (b) applies because Applicant was not authorized to store Contractor A's proprietary information on his home computer. The agreement Applicant signed when he became an employee of Contractor A clearly stated that this was prohibited without prior written approval from Contractor A. Applicant should have known what the rules were with regard to protecting Contractor A's proprietary information.

AG ¶ 34(c) applies because Applicant transferred some of Contractor A's proprietary information to his home computer which was not approved for use by Contractor A. AG ¶ 34(g) applies because Applicant failed to comply with the Contractor A's rules for protecting proprietary information.

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.

AG ¶¶ 35(a) and 35(b) apply to Applicant's case. More than five years have passed since Applicant's termination from Contractor A. While Applicant's conduct was grossly negligent, he has since demonstrated that he can be trusted to handle classified information. He has handled both Secret and Top Secret information with his subsequent employers, Contractor C and Contractor D. His current supervisor at Contractor D testified on his behalf and lauded his security awareness. While his supervisor was aware of the incident at Contractor A, he recommended that Applicant be allowed to keep his security clearance based on his experience of working directly with Applicant on a daily basis for three years. Applicant's conduct at Contractor A does not cast doubt on his current reliability, trustworthiness, and judgment.

AG ¶ 35(b) applies because Applicant cooperated with Contractor A when they discovered the file transfer. Since that time, he has been steadfast in protecting classified information with his subsequent employers. While Applicant was not offered remedial security training, he has learned a difficult lesson. He was fired immediately from his position at Contractor A. Contractor B withdrew their job offer. Applicant was unemployed for several months and had to accept a job that resulted in a 25 percent reduction in his previous income. Despite this, he has demonstrated a positive attitude toward the discharge of his security responsibilities.

Applicant mitigated the concerns raised under Guideline K.

**Guideline M – Use of Information Technology Systems**

The concern under this guideline is set out in AG ¶ 39:

> 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.

The following disqualifying conditions are potentially relevant:

AG ¶ 40(a): illegal or unauthorized entry into any information technology system or component thereof;

AG ¶ 40(b): illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;

AG ¶ 40(c): use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

AG ¶ 40(d): downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;

AG ¶ 40(e): unauthorized use of a government or other information technology system;

AG ¶ 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;

AG ¶ 40(g): negligence or lax security habits in handling information technology that persist despite counseling by management; and

AG ¶ 40(h): any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

I find AG ¶ 40(f) applies to Applicant's case. When he chose to transfer files containing Contractor A proprietary information to his home computer's hard drive, it was clearly against the rules. When he started work at Contractor A, he signed an agreement which expressly stated: "I further agree not to make electronic or hard copies of any Proprietary Information, except as authorized in writing by the Company." Applicant did not seek authorization before transferring Contractor A's proprietary information to his home computer even though he should have been aware of the rules for protecting Contractor A's proprietary information.

The following mitigating conditions under Guideline M are potentially relevant:

> AG ¶ 41(a): so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
>
> AG ¶ 41(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
>
> AG ¶ 41(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.

AG ¶ 41(a) applies because it has been five years since Applicant's termination from Contractor A. During this time, Applicant has demonstrated that he can be trusted to handle classified information based on his positive performance evaluations with his subsequent employers and the favorable opinion by Mr. P., his current supervisor, on his ability to handle classified information and follow security procedures.

**Guideline E – Personal Conduct**

The security concern relating to the guideline for Personal Conduct is set out in AG ¶15:

> 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.

With respect to SOR ¶3.a which cross alleges the allegations under Guideline K, SOR ¶¶ 1.a and 1.b, the following disqualifying conditions potentially apply to Applicant's case:

> AG ¶ 16(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;
(4) Evidence of significant misuse of Government or other employer's time or resources; and

AG ¶ 16(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

AG ¶ 16(d)(3) applies because Applicant violated Contractor A's rules regarding proprietary information when he transferred files, some of which contained proprietary information to his home computer using a personal thumb drive. He did not seek permission before transferring these files. Applicant also certified in April 2012 that he did not have Contractor A company proprietary information in his possession, when he still had Contractor A proprietary information on his computer. This demonstrates a pattern of dishonesty and rule violations.

Appellant's actions also violated Contractor A's Non-Disclosure and Invention Assignment Agreement that Applicant signed in July 2008, when he was hired by Contractor A. As a result, AG ¶ 16(f) applies Applicant violated his commitment to protect Contractor A's proprietary information. As a condition of his employment, he committed to protecting Contractor A's proprietary information.

With respect to SOR ¶ 3.a, the following mitigating conditions have the potential to apply under personal conduct:

AG ¶ 16(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; and

AG ¶ 16(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.

Both AG ¶ 16(c) and AG ¶ 16(d) apply. Five years have passed since the incident at Contractor A. Since that time, Applicant has worked for two other defense contractors. His duties required handling both Secret and Top Secret information. His performance reviews were favorable. His current supervisor recommends that he continue to have access to classified information. Applicant admits that he should have followed proper protocols when transferring some of his files from the Contractor A computers. I find his explanation that he did not intend to use Contractor A's proprietary

information for subsequent job opportunities to be credible. He intended to transfer files that were not proprietary and hoped to delete the files before he left the company. His actions were grossly negligent, but his intentions were without malice. Applicant said he learned a difficult lesson about handling information. His current supervisor attests that Applicant is meticulous about protecting classified information. A significant amount of time has passed since Applicant's termination from Contractor A. He acknowledged his behavior and has since demonstrated that he is trustworthy to handle classified information.

With regard to the falsification allegation in SOR ¶ 3.b, the following disqualifying condition potentially applies:

> AG ¶ 16(b) directly providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative.

For AG ¶ 16(b) to apply, Applicant's falsifications have to be deliberate. Applicant has always maintained that he incorrectly transferred the files from his work computer to his home computer. He was attempting to transfer some of his personal documents but the files he transferred also contained proprietary information. Applicant admits to being aware that he some of the files contained proprietary information. Applicant incorrectly transferred the files, but had no intent to retain the files. He intended to delete the proprietary files before he left Contractor A's employment. He just went about this process in a careless and sloppy manner. While Applicant's actions certainly look bad and were grossly negligent, there is no proof that he had an ulterior motive to use Contractor A's proprietary information at his new employer. Applicant fully cooperated with the investigation by Contractor A. He also cooperated with the investigators conducting his security clearance background check. I find he did not provide false or misleading information to the investigator conducting his background investigation interview. His testimony to the investigator was taken out of context.

**Whole-Person Concept**

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all 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.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. Applicant is highly respected by current and former supervisors. He is a family man who has worked over 30 years as a DOD contractor. During this time, he made a valuable contribution to the war effort. His decision to transfer Contractor A files using his personal thumb drive to his home computer was very irresponsible and grossly negligent, however, there is no evidence that he intended to use this information for ill gotten gains. Applicant merely chose a careless way to transfer his personal files. I note that Applicant cooperated fully during the investigation. I note that DSS was involved in the investigation and determined there was no breach of security and no classified information was compromised. I considered that Applicant's security clearance was reinstated after the conclusion of the investigation.

Applicant also did not read the Termination Certification carefully before signing it, because he was leaving on vacation. He understands he should have read it more carefully and has learned to be more careful in the future. One has to wonder why Contractor A needed him to sign the Termination Certification on April 5, when he had three more weeks of employment with them. Applicant did not use the best judgment when transferring files that he believed to be his to his home computer and when hastily signing the Termination Certificate. He apologized for his actions and said it was a valuable learning experience.

As a result of his negligence in handling Contractor A's proprietary information, Applicant was immediately terminated from Contractor A. He was unemployed for several months because Contractor B withdrew their employment offer after being contacted by Contractor A. He accepted a job that offered a 25 percent reduction in income. Applicant endured hardship as a result of his actions. The incident taught him a valuable lesson about protecting proprietary information. Over the past five years, Applicant has worked for two additional DOD contractors and has handled both Secret and Top Secret information without incident. Security concerns are mitigated.

## 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 K: | FOR APPLICANT |
| Subparagraph 1.a: | For Applicant |

| | |
|---|---|
| Subparagraph 1.b: | For Applicant |
| Paragraph 2, Guideline M: | FOR APPLICANT |
| Subparagraph 3.a: | For Applicant |
| Paragraph 3, Guideline E: | For APPLICANT |
| Subparagraph 3.a: | For Applicant |
| Subparagraph 3.b: | For Applicant |

## Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
ERIN C. HOGAN
Administrative Judge