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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| ---------- | ) | ISCR Case No. 17-02998 |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Aubrey De Angelis, Esq., Department Counsel
For Applicant: Ronald C. Sykstus, Esq.

04/12/2019

_____

## Decision

_____

LEONARD, Michael H., Administrative Judge:

Applicant contests the Defense Department's intent to revoke his eligibility for access to classified information. He did not provide sufficient evidence to mitigate the security concerns stemming from his intentional destruction of a company-owned external hard drive to which he had transferred or moved approximately 1,600 files, which included company propriety information, in advance of beginning another job in the defense industry. Accordingly, this case is decided against Applicant.

## Statement of the Case

Applicant completed and submitted a Standard Form (SF) 86, Questionnaire for National Security Positions, the official form used for personnel security investigations, on January 22, 2016.[1] This document is commonly known as a security clearance application. Thereafter, on October 9, 2017, after reviewing the application and the information gathered during a background investigation, the Department of Defense

[1] Exhibit 1.

Consolidated Adjudications Facility, Fort Meade, Maryland, sent Applicant a statement of reasons (SOR), explaining it was unable to find that it was clearly consistent with the national interest to grant him eligibility for access to classified information. The SOR is similar to a complaint. It detailed the factual reasons for the action under the security guidelines known as Guideline K for handling protected information, Guideline M for use of information technology, and Guideline E for personal conduct. Although the SOR alleged three security guidelines, the factual allegations at issue are set forth in SOR ¶¶ 1.a and 1.b and then simply cross-alleged in SOR ¶¶ 2.a and 3.a.[2]

Applicant answered the SOR on October 26, 2017, in a four-page memorandum. His answers were mixed and included detailed explanations. He also requested a hearing before an administrative judge.

The case was assigned to me on November 17, 2017. The hearing did not take place as scheduled on January 25, 2018, due to a government shutdown. The hearing took place as rescheduled on April 20, 2018. Applicant appeared with counsel. Department Counsel offered documentary exhibits, which were admitted as Exhibits 1 and 2, and called no witnesses. Applicant offered documentary exhibits, which were admitted as Exhibits A - LL, and called eight witnesses in addition to his own testimony. The hearing transcript (Tr.) was received on May 8, 2018.

## Ruling on Evidence

Both of Department Counsel's exhibits, Exhibits 1 and 2, were admitted without objections.[3] Nevertheless, some commentary on Exhibit 2 is appropriate.

Exhibit 2 contains records from Applicant's former employer and consists of two parts. The first part is three pages of human resources information reflecting dated entries (e.g., new hire, merit increase, change in reports, etc.) concerning Applicant's employment with the company, which ended on December 18, 2015, with a determination that Applicant was ineligible for rehire due to the reasons of "ethics/HR/legal/security inv." By all appearances, the three pages constitute a business record made at or near the time of the events described and kept in the course of regularly conducted business activity, which would normally be admissible under the rules that govern these cases.[4]

[2] At the start of the hearing, the parties were informed that the factual allegation in SOR ¶ 1.c did not allege any independent disqualifying matters, but instead alleged a consequence or result of the conduct alleged in SOR ¶¶ 1.a and 1.b. Therefore, the parties were informed that I would not consider the allegation for disqualification purposes, but would consider it as a relevant fact in terms of assessing the seriousness of the underlying behavior. Neither Department Counsel nor Applicant raised an objection. Tr. 11-12. Accordingly, SOR ¶ 1.c is decided for Applicant on that basis.

[3] Tr. 14-15.

[4] *See* Federal Rule of Evidence 803(6).

The second part of Exhibit 2 is a two-page memorandum prepared by a company official located in a distant state from where Applicant lived and worked when employed by the company.[5] The memorandum is dated January 23, 2018. It describes the employer's investigation of events that occurred more than two years earlier in December 2015. In other words, it was not made at or near the time of the events described. Given the date of the document, it is obvious that the memorandum was prepared for the purpose of litigation in this case, which was initially scheduled to be heard on January 25, 2018, two days after the date of the memorandum. The memorandum is not self-authenticating, and it was not authenticated by a witness at the hearing.[6] In addition, Applicant did not have an opportunity to cross-examine the person who prepared the memorandum. Although the exhibit was admitted without objections, I will weigh the January 23, 2018 memorandum in light of the matters discussed above.

## Findings of Fact

Applicant is a 57-year-old employee who is seeking to retain a security clearance in the defense industry. He also held a security clearance during previous military service. He is employed as a facility clearance officer (FSO) for a company doing business in the defense industry. He also has two part-time jobs that are not at issue in this case.[7] His formal education includes two associate's degrees, a bachelor's degree awarded in 2008, and a master's degree in business administration in 2011. His first marriage ended in divorce in 1990, and he has been married to his second spouse since 1990. He has eight adult children, none of whom live in his household.

Applicant comes from a military family. His father retired after 30 years of military service. His wife is a retired servicemember too. Applicant served on active military duty from 1982 until he retired in 2005. He worked in the fields of law enforcement and security services. He spent the last five years working in industrial information and personnel security where he was also responsible for protecting classified information and equipment.[8] He has a 20% disability rating from the Department of Veterans Affairs. He next worked as an FSO for a company during 2005-2011. He also had about eight months as a self-employed security consultant in 2011. He began his employment as an FSO and the contract program security office (CPSO) for his previous employer in July 2011. His employment ended in December 2015, the circumstances of which form the basis for the SOR allegations.

[5] Applicant testified that he was unfamiliar with the person who prepared Exhibit 2. Tr. 63-64.

[6] Directive, Enclosure 3, ¶ E3.1.20 requires authenticating witnesses under certain circumstances, such as when the documentary exhibit in question was not furnished by an investigative agency pursuant to its responsibilities in connection with assisting the Secretary of Defense to safeguard classified information within industry.

[7] Tr. 67-68.

[8] Tr. 22-23.

Applicant has an excellent employment record and a good reputation in his line of work. He presented substantial documentary evidence establishing his honorable military service, his past job performance, and training in occupational specialty.[9] In addition, he called eight witnesses all of whom vouched for his overall professionalism, knowledge of the job, reliability, trustworthiness, and good judgment. In particular, I was especially impressed by the testimony of a witness who is employed as a special agent working in the field of industrial security for the Defense Security Services. The witness described Applicant's work as a FSO as "very exceptional" with a lot of knowledge and expertise.[10]

Turning to the SOR allegations, two matters are at issue stemming from his employment as an FSO, which ended in December 2015. First, the SOR alleges Applicant mishandled company proprietary information in 2015 when he transferred over 1,600 files, including company proprietary information, to a company-approved external hard drive without authorization. Second, the SOR alleges that during the course of the 2015 investigation into the above matter, he was asked to return the external hard drive in question, but intentionally returned another external hard drive, and he then intentionally and without authorization destroyed the external hard drive containing company proprietary information.

Applicant has provided varying accounts of his involvement in the 2015 incident. In his January 2016 security clearance application, he said he left his job as an FSO in December 2015 because he received notice on November 30, 2015, that the contract was ending and he resigned on December 18, 2015.[11] That is consistent with the layoff notice his employer provided with a last day of work scheduled for February 5, 2016, and Applicant's December 3, 2015 letter of resignation with an effective date of December 18, 2015.[12] He denied leaving the job under adverse circumstances.

But in response to Question 27 of the application, concerning use of information technology systems, he admitted in the last seven years illegally or without authorization, modifying, destroying, manipulating, or denying others access to information residing on an information technology system or attempted to do the same.[13] He then provided the following comments and explanation concerning his affirmative answer to Question 27:

> I will attempt to explain my answer to the question in more detail. I had given [employer] my two week notice for two reasons, one was [the] contract was ending in February 2016, and two because I was offered

[9] Exhibits A – FF.

[10] Tr. 136.

[11] Exhibit 1 at 14-15.

[12] Exhibits GG and HH.

[13] Exhibit 1 at 56.

> another position with another company. During that two week period, I was cleaning out my files and paperwork, and also transferring some of my accounts to other [company] employees who was taking over my positions. On Dec. 16, 2015, I was asked by [employer] to turn over the [external] hard drive I was downloading stuff to. I explained that the hard drive had personal[ly] identifiable information (PII) on it. I turned a different [external] hard drive that I had in my possession and destroyed the hard drive that had PII on it. I destroyed the hard drive that contained my personal information because I did not want to provide my personal information to unknown personnel such as my [SF 86], a few "prescreening questionnaires" for another program, and other PII data. When asked, I explained that I knowingly provided my [employer] a [external hard] drive that did not have personal data and that I destroyed [the external hard] drive that contained PII. I was then informed that I destroyed the hard drive without authorization.[14]

He offered additional details about the incident in response to another question as follows:

> [I] destroyed a company [external] hard drive [known as a] Passport that was issued to me sometime in 2012. I had personal information on the hard drive including my social security number on documents and other personal items that I did not want to leave behind at the company.[15]

He further stated that he was relieved of duty with pay on December 16, 2015, and his last day of work with the company was December 18, 2015.

Applicant addressed both SOR allegations in his written answer. He formally denied the allegation in SOR ¶ 1.a. He explained that he transferred files from a company-approved laptop to a company-approved external hard drive, the purpose of which was to "sanitize" the laptop of PII and other files he had compiled over the course of four years of employment with the company.[16] He further explained that his actions were driven by the unusual circumstance of the company layoff notice he received on December 15, 2015.

Concerning the allegation in SOR ¶ 1.b, Applicant admitted providing an incorrect external hard drive and intentionally destroyed the external hard drive in question. He explained that he was acting in good faith to ensure that he did not improperly or inadvertently release PII, such as social security numbers, addresses, identifications, etc. He denied knowing if any company proprietary information was on the destroyed

[14] Exhibit 1 at 56-57.

[15] Exhibit 1 at 57. The parties sometimes referred to the external hard drive as a Passport during the hearing. I refer to Passport #1 and Passport #2 to distinguish between the two external hard drives.

[16] Applicant explained that his definition of sanitize meant extracting information. Tr. 74.

hard drive, but said any such information was certainly backed-up on the shared drive at work and easily accessible in that way.

In his hearing testimony, Applicant described the events leading up to his decision to accept a new job and give two weeks' notice to his then employer. He then explained that he was confronted by a company official about downloading information during a telephone call setup as a debriefing.[17] He denied downloading information to a personal hard drive or personal USB drives.[18] He also denied downloading any proprietary information.[19] The call ended that day on December 16, and Applicant went to another location to assist the work there. While there he received another call from the company to inform him that he was relieved from duty, and he was instructed to turn over his company-owned property (e.g., badge, keys, laptop, etc.).[20] He did as instructed and then got into his car and went home.

Applicant destroyed a company-owned external hard drive (Passport #1) after arriving home.[21] He explained that he dismantled it with tools, put the parts in his grill, and burned the parts with the assistance of lighter fluid. He explained that Passport #1 ended up at his home because he routinely carried it in a bag due to its sensitivity, and the bag was in his car when he went home that day. He agreed that Passport #1 contained sensitive but unclassified information. He stated that as far as he knew Passport #1 did not contain any company proprietary information. He stated that it did not occur to him to turn in Passport #1 with the other equipment at the worksite because he was surprised and in shock about being relieved from duty. Upon arriving home, he realized he had Passport #1 and was concerned about it. Knowing Passport #1 contained PII associated with other people, he decided to destroy the device. It did not occur to him at the time to call his supervisor at work and inform them about his possession of Passport #1. He thinks he may have called someone at work subsequently and was unable to talk with anyone, but he does not remember with certainty.

The investigation by Applicant's former employer substantiated the allegations of damage to the company's assets and unauthorized downloads.[22] Applicant along with the other employees who received layoff notices at the end of November 2015 were placed on elevated computer and e-mail monitoring. In addition, a 90-day retroactive download report was generated that showed Applicant had conducted multiple downloads to a "possible personal external device," since September 2015, with more

[17] Tr. 33-34.

[18] Tr. 34.

[19] Tr. 34.

[20] Tr. 34-35.

[21] Tr. 55-56, 68-71.

[22] Exhibit 2 at 4-5 (the following five paragraphs rely on the January 23, 2018 memorandum prepared by Applicant's former employer).

than 1,600 files being moved, to include presumed personal files and company files that likely contained company proprietary information (e.g., security-related forms, presentations, templates, and letters).

Company investigators interviewed Applicant on Wednesday, December 16, 2015, which was a couple of days before Applicant's final day of work on December 18. Applicant admitted using the external hard drive for work-related matters but not for personal use. When confronted that computer data showed that personal information was on the device, Applicant stated he did not know what they were talking about. Applicant stated that it was a company-purchased device that was given to him by another employee. He also stated that he used the device for work-related tasks while at the site or on business travel and had done so for the last three years. Applicant indicated that he would turn over the device to his manager before his departure from the company. He further stated that he did not have any classified or proprietary information in his possession.

After the interview, Applicant was placed on paid administrative leave for the remaining two days of his two-week-notice period. Applicant turned over all assigned company assets to security, and Passport #2 was turned over to the site manager for review.

The company determined that the external hard drive was only used with Applicant's company-issued laptop. They also determined that the contents of Passport #2 were different from the files displayed in the screenshots and it was not the device Applicant used for downloads and during the monitoring period.

Applicant was contacted again concerning Passport #1. He stated that he had two Passports while at work, but he withheld this information, although he knew the company investigator wanted to obtain Passport #1. Applicant stated that he did not want anyone having access to his personal information on Passport #1. He further stated that he brought Passport #1 to his home and destroyed it even though he knew the device was company property and should have been returned to the company for review. He described how he destroyed the device by dismantling it and burning the parts in his grill. He further stated that he did not have any classified or property information in his possession, and he apologized for deceiving the company investigator during the interview. The memorandum ends by noting that Applicant resigned in lieu of termination on December 18, 2015.

Based on the matters set forth above, I hereby make the specific findings of fact:

1. Applicant mishandled company proprietary information in 2015 by transferring or downloading more than 1,600 files, including company propriety information, to a company-approved external hard drive (Passport #1) without authorization.

2. Applicant was asked to return the external hard drive (Passport #1) containing the company proprietary information during the 2015

company investigation, but he instead returned another external hard drive (Passport #2) while at the same time retaining and destroying the sought-after device (Passport #1). Destruction of the device was intentional and without authorization from his then employer.

## Law and Policies

This case is adjudicated under Executive Order (E.O.) 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 *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AG), effective June 8, 2017.[23]

It is well-established law that no one has a right to a security clearance.[24] As noted by the Supreme Court in *Department of the Navy v. Egan*, "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."[25] Under *Egan*, Executive Order 10865, and the Directive, any doubt about whether an applicant should be allowed access to classified information will be resolved in favor of protecting national security. In *Egan*, the Supreme Court stated that the burden of proof is less than a preponderance of evidence.[26] The Appeal Board has followed the Court's reasoning, and a judge's findings of fact are reviewed under the substantial-evidence standard.[27]

A favorable clearance decision establishes eligibility of an applicant to be granted a security clearance for access to confidential, secret, or top-secret information.[28] An unfavorable clearance decision (1) denies any application, (2) revokes any existing security clearance, and (3) prevents access to classified information at any level.[29]

There is no presumption in favor of granting, renewing, or continuing eligibility for access to classified information.[30] The Government has the burden of presenting

[23] The 2017 AG are available at http://ogc.osd.mil/doha.

[24] *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988) ("it should be obvious that no one has a 'right' to a security clearance"); *Duane v. Department of Defense*, 275 F.3d 988, 994 (10th Cir. 2002) (no right to a security clearance).

[25] 484 U.S. at 531.

[26] 484 U.S. at 531.

[27] ISCR Case No. 01-20700 (App. Bd. Dec. 19, 2002) (citations omitted).

[28] Directive, ¶ 3.2.

[29] Directive, ¶ 3.2.

[30] ISCR Case No. 02-18663 (App. Bd. Mar. 23, 2004).

evidence to establish facts alleged in the SOR that have been controverted.[31] An applicant is responsible for presenting evidence to refute, explain, extenuate, or mitigate facts that have been admitted or proven.[32] In addition, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.[33]

## Discussion

Although the SOR alleges three different security guidelines, Guidelines K, M, and E, they rely on the same set of facts and circumstances as set forth in the initial paragraphs of the SOR at ¶¶ 1.a and 1.b. Given these circumstances, these matters will be addressed together, because the overall decision is an evaluation of Applicant's trustworthiness, judgment, reliability, and willingness and ability to safeguard protect classified or sensitive information, which are central matters for consideration under all three security guidelines.

Under Guidelines K, M, and E, I have considered the following disqualifying conditions as most pertinent to the facts and circumstances of this case: AG ¶¶ 34(b) and (g), AG ¶¶ 40(b) and (d), and AG ¶ 17(c). Likewise, under Guidelines K, M, and E, I have considered the following mitigating conditions as most pertinent to the facts and circumstances of this case: AG ¶ 35(a), AG ¶ 41(a), and AG ¶ 17(c). Having considered the totality of facts and circumstances in light of the pertinent disqualifying and mitigating conditions, I conclude that Applicant did not provide sufficient evidence to mitigate the security concerns stemming from his intentional destruction of a company-owned external hard drive to which he had transferred or moved approximately 1,600 files, which included company propriety information, from his company-owned laptop in advance of beginning another job in the defense industry. The sheer number of downloaded files, reported to be more than 1,600, supports a conclusion Applicant was transferring more than personal files.

My main concerns and doubts in this case are twofold. First, Applicant gave varying accounts of his involvement in the 2015 incident. Taken as a whole, his accounts are at variance in important respects with his former employer's account of the 2015 investigation as set forth in the January 2018 memorandum. For example, according to the January 2018 memorandum, Applicant admitted that he purposely provided Passport #2 instead of Passport #1 to company officials. He said essentially the same thing in his January 2016 security clearance application, as quoted in the findings of fact. But in his hearing testimony he attributed his retention of Passport #1 to oversight during the unexpected circumstance of being relieved from duty on December

[31] Directive, Enclosure 3, ¶ E3.1.14.

[32] Directive, Enclosure 3, ¶ E3.1.15.

[33] Directive, Enclosure 3, ¶ E3.1.15.

16. Given the varying accounts, I am uncertain if Applicant is giving full, frank, and truthful answers about his involvement in this matter.[34]

Second, Applicant did not conduct himself as an honest person on December 16 knowing that he still had Passport #1. An honest person would have made a reasonable effort to return Passport #1 to his employer. Return of the device could have been accomplished by a telephone call or e-mail to his supervisor or some other company official; getting in the car and returning the device to his employer's worksite; or by mailing or delivery of the device to the employer along with an explanatory note. Applicant thinks he may have made a phone call without success, but his recollection is uncertain. Further, an honest person would not have rushed to destroy Passport #1 on the same day he was placed on administrative leave, knowing that it was likely the company would be looking for it. Other than a single phone call, he did none of things an honest person would have done if they had inadvertently or mistakenly retained Passport #1. Instead, Applicant destroyed Passport #1 by dismantling it with tools and burning the parts in his grill. Such conduct is suspicious and suggests he was trying to hide or conceal adverse information. Given these circumstances, I view Applicant's transgressions as reflected herein to be serious misconduct.

Following *Egan* and the clearly consistent standard, I have doubts and concerns about Applicant's reliability, trustworthiness, good judgment, and ability to protect classified or sensitive information. In reaching this conclusion, I weighed the evidence as a whole and considered if the favorable evidence outweighed the unfavorable evidence or *vice versa*. I also considered the whole-person concept. In doing so, I considered Applicant's 23-plus years of honorable military service, his years of holding a security clearance in the military and while working in the defense industry, his excellent employment record, his formal education, his wealth of training in his occupational speciality, and the highly favorable testimony of the eight witnesses. Nevertheless, his favorable evidence does not outweigh the seriousness of his misconduct. Accordingly, I conclude that he did not meet his ultimate burden of persuasion to show that it is clearly consistent with the national interest to grant him eligibility for access to classified information.

## Formal Findings

The formal findings on the SOR allegations are:

| | |
|---|---|
| Paragraph 1, Guideline K: | Against Applicant |
| Subparagraphs 1.a - 1.b: | Against Applicant |
| Subparagraph 1.c: | For Applicant |
| Paragraph 2, Guideline M: | Against Applicant |

[34] Directive, ¶ 6.2 ("An applicant is required to give . . . full, frank, and truthful answers to relevant and material questions needed by DOHA to reach a clearance decision and to otherwise comply with the procedures authorized by this Directive.").

| | |
|---|---|
| Subparagraph 2.a: | Against Applicant |
| Paragraph 3, Guideline E: | Against Applicant |
| Subparagraph 3.a: | Against Applicant |

## Conclusion

It is not clearly consistent with the national interest to grant Applicant access to classified information. Eligibility denied.

Michael H. Leonard
Administrative Judge