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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| | ) | ISCR Case No. 22-02423 |
| | ) | |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: William H. Miller, Esq., Department Counsel
For Applicant: Christopher Snowden, Esq.

04/12/2024

_____

## Decision

_____

HOGAN, Erin C., Administrative Judge:

On February 1, 2023, the Defense Counterintelligence and Security Agency Consolidated Adjudication Services (DCSA CAS) issued a Statement of Reasons (SOR) to Applicant detailing the security concerns under Guideline K, Handling Protected Information; and Guideline E, Personal Conduct. The action was taken under Executive Order (EO) 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 the Department of Defense on June 8, 2017.

On February 21, 2023, Applicant answered the SOR and requested a hearing before an administrative judge. The case was assigned to me on September 8, 2023. On December 15, 2023, a Notice of Hearing was issued, scheduling the hearing on January 16, 2024. The hearing was held as scheduled. During the hearing, the Government offered three exhibits, which were admitted without objection as Government Exhibits (GE) 1 - 3. Applicant testified and offered eight exhibits, which were admitted without objection as Applicant Exhibits (AE) A - H. After the hearing, he submitted an additional exhibit which was admitted without objection as AE I. The transcript was received on January 24, 2024. Based upon a review of the case file, pleadings, and exhibits, eligibility for access to classified information is granted.

## Procedural Issue

During the hearing, Department Counsel moved to amend SOR ¶ 1.b pursuant to the Directive ¶ E3.1.17, as follows:

> You improperly took home a printed e-mail that contained protected information. When you surrendered the e-mail at a nearby SCIF in 2020, you declined to file a formal report.

Applicant's counsel had no objection. The amendment was approved. (Tr. 96 – 99)

## Findings of Fact

In his answer to the SOR, Applicant admitted to the allegations in the SOR ¶¶ 1.a, 1.b, and 2.b, and denied the allegation in SOR ¶ 2.a.

(Note: Some details were excluded to protect the privacy of Applicant and other individuals named in the record. Specific information is available in the cited exhibits and transcript.)

Applicant is a 68-year-old employee of a DOD contractor who seeks to maintain a security clearance. He has held a security clearance off and on over his 30-year career. His highest level of education is a bachelor's degree. His first wife passed away in 2005. He remarried in 2007. He has four adult children. (Tr. 42-43; GE 1; GE 2; AE F)

On December 2, 2019, Applicant completed an electronic questionnaire for investigations processing (e-QIP) in order to apply for a security clearance. (GE 1) A subsequent background investigation raised the security concerns listed in the SOR.

Under the Guideline K – Handling Protected Information security concern, the SOR alleged Applicant, in or around 2007, improperly took home a classified cover sheet. Instead of returning the cover sheet and reporting the incident, he destroyed the cover sheet by tearing it into little pieces and consuming them. (SOR ¶ 1.a: GE 3 at 9-10). He improperly took home a printed e-mail that contained protected information. When he surrendered the e-mail at a nearby SCIF in 2020, he declined to file a report. (SOR ¶ 1.b: GE 3 at 10-11).

Under the Guideline E – Personal Conduct security concern, the SOR alleged: Applicant failed to fully and timely report or disclose the conduct in subparagraphs 1.a and 1.b (SOR ¶ 2.a: GE 3 at 9-11); and he was terminated from his employment with Contractor A after the government customer requested he be removed from their project. (SOR ¶ 2.b: GE 1 at 15-16; GE 3 at 7)

In 2007, Applicant was a federal contractor working at Government Agency #1. While working there, he often printed unclassified e-mails, unclassified documents, and unclassified power point slides. He took them home to use for work or for scrap paper to write notes on. One day, he printed out a handful of unclassified documents to use as

scrap paper. After printing out the documents, he left work and drove home. Once he arrived home, he went to his office to do some work. When going through the unclassified documents he had just brought home, he discovered a classified cover sheet from the printer where he printed his unclassified documents. He claims it was an unclassified printer and the cover sheet did not contain classified information, but there was a statement on the cover sheet stating to treat the cover sheet as classified information. (Tr. 21-24; GE 3 at 9, 22-23, 51)

Applicant decided to tear up the cover sheet into little pieces and ate it rather than turning it into the office and reporting the incident. He chose to eat the document because he assumed it would be unrecoverable. He claims this was his first job involving classified information and that he was not trained on how to handle this incident. He never reported the incident to his security officials or supervisor. He did not remember whether he had a duty to report this incident. In 2018 or 2019, he underwent a polygraph exam with Government Agency #2. He was applying for Top Secret – Sensitive Compartmented Information (TS-SCI) access. He failed the polygraph. The polygrapher asked him if there was anything that caused him to fail the polygraph. He told the polygrapher about the 2007 incident where he swallowed the classified cover sheet. He is embarrassed about this incident. He handled it poorly and apologized. In hindsight, he should have taken the fax cover sheet back to the office and told his supervisor. (Tr. 23-26, 47-57; GE 3 at 9-10, 21-23)

Shortly after this polygraph, Applicant began to destroy the unclassified documents that he took home from various work sites. He had over 1,000 pages of unclassified documents at his home. In April 2020, while cleaning out documents, he discovered an e-mail from the 2007 timeframe that he had marked as Confidential. He immediately became concerned and took the document and surrendered it to the nearest Sensitive Compartmented Information Facility (SCIF), which was located at a military installation. He stopped at the main gate and informed the security police that he wanted to turn a classified document into the SCIF. He had to wait for a person who held a security clearance and had access to the SCIF. When the person arrived, Applicant explained how he discovered the document and that he thought it best to surrender it to the SCIF for safekeeping. He was there for over an hour, possibly two. At the end of discussions, he was asked if he would like to make a formal report. He declined, indicating that he provided them the information and did not want to take up any more of their time. He stated one of the military policemen told him informally that he should have just shredded the document. He did not know that he was required to make a formal written report. He understood the report to be optional. There is nothing in the record indicating that he was required to make a formal written report. (Tr. 27-34, 59-66; GE 3 at 9, 23-24; AE A)

Applicant describes both incidents as accidents. He believes that he had over-classified the e-mail involved in the 2020 incident out of an abundance of caution. He also printed out unclassified documents to take home because they showed his accomplishments on various projects that he worked on. He has since destroyed all of the unclassified documents that he brought home and no longer prints out any unclassified documents to take home. He claimed it was more common to print out documents back then than it is today. (Tr. 66-67)

Applicant listed on a December 2019 security clearance application that he was terminated from his employment with Contractor A while working on a contract with Government Agency #3 in April 2018. He was never told why his position on the contract ended and does not believe he did anything wrong. All he was told is that he was removed from his position at the request of the government customer. Contractor A attempted to find a position for him on another government contract but was unsuccessful. On April 16, 2018, they terminated his employment. They indicated that they enjoyed having him as a member of the team, appreciated his hard work, and wished him the best of luck in his future endeavors. Applicant was unemployed for about a month. He easily found employment with another contractor. (Tr. 34-39, 73-79; GE 1, section 13A at 15-16; AE B; AE C)

**Whole-person Evidence**

Mr. M., a government customer, wrote an e-mail to the contractor who employed Applicant in 2022 praising his duty performance. He said he was impressed with Applicant's "level of detail, expert knowledge, peer mentoring support, and overall performance." Mr. M. was grateful to have his thoughtful risk analysis and broader technical experience to help him make decisions for the organization. He indicated Applicant was "our best contractor staff." (AE I)

**Unalleged Conduct**

The following incidents were raised during the hearing. They are not alleged in the SOR. I consider each instance under matters of extenuation and mitigation and not as matters of disqualification.

During the hearing, Applicant volunteered that he two minor incidents involving walking into a SCIF with his cell phone between 2017 and 2019. The first time occurred between 2017 and 2018, he was going to a meeting in a SCIF and forgot to put his cell phone in a cell phone receptacle outside the SCIF. He felt his pocket after going through a turnstile. He had not entered the SCIF. He immediately turned around and put his cell phone in a cell phone receptacle. The second time occurred between 2018 and 2019, he forgot to put the cell phone in a cell phone receptacle before entering the SCIF. He discovered he still had his cell phone before the start of the meeting. He immediately went outside the SCIF to put his cell phone in a cell phone receptacle. (Tr. 72-73, 91-94) Both incidents are similar, relatively minor and appear to have been oversights that Applicant caught before entering the SCIF and/or before the classified meeting in the SCIF began. It is highly unlikely classified information was compromised.

Applicant also testified during the hearing that he was abruptly terminated from contracts with five different employers. (Tr. 82-84) It is unclear whether there was any misconduct or security issues on Applicant's part in each of these instances. There is no evidence that any of the employers or government customers filed a security incident report.

## 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 overarching adjudicative goal is a fair, impartial and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for national security eligibility 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.

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 EO 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).

**Guideline K, Handling Protected Information**

The security concern relating to the guideline for Handling Protected Information is set out in AG ¶ 33:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information – which includes classified and other sensitive government information, and proprietary information – raises doubt about an individual's trustworthiness, judgment, and reliability, or willingness and ability to safeguard such information, and is a serious security concern.

AG ¶ 34 notes several disqualifying conditions that could raise security concerns. The following potentially apply to Applicant:

> AG ¶ 34(b) collecting or storing protected information in any unauthorized location; and
>
> AG ¶ 34(g) any failure to comply with rules for the protection of classified or sensitive information.

AG ¶ 34(b) and AG ¶ 34(g) apply. The evidence supports that Applicant stored classified information at home. While inadvertent, he was not authorized to take and store classified information at home. He also failed to comply with the rules pertaining the protection of classified and sensitive information when he chose to tear into little pieces and eat the classified cover sheet in 2007. He also failed to insure that the documents that he took home during that time did not include classified information. Thirteen years later, he discovered that he had taken home an e-mail that was marked Confidential that was mixed in with the unclassified documents that he took home. During his career, Applicant took home up to 1,000 documents. It is not clear whether any of these documents were sensitive. Upon discovering the Confidential e-mail, Applicant's decision to turn the document into the closest SCIF from his house was prudent. He fully disclosed how he came to possess the confidential document to the officials at the base where he surrendered the document. There is nothing in the record that indicates he was required to file a formal report.

The Government's substantial evidence and Applicant's own admissions raise security concerns under Guideline K, Handling Protected Information. 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 also includes examples of conditions that could mitigate security concerns arising from Handling Protected Information. The following mitigating conditions potentially apply to the Applicant's case:

AG ¶ 35(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;

AG ¶ 35(c) the security violations were due to improper or in adequate training or unclear instructions; and

AG ¶ 35(d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

AG ¶ 35(a) applies with respect to SOR ¶ 1.a, more than 17 years have passed since Applicant discovered he inadvertently took home a classified cover sheet. There remains a question as to whether the cover sheet itself was classified. While Applicant should have returned the cover sheet to the office and informed his supervisor or security officer of what happened, it was an unusual occurrence.

AG ¶ 35(a) also applies with respect to SOR ¶ 1.b. Applicant inadvertently took home a paper that was classified as Confidential in 2007. It was mixed in with many other unclassified documents that he took home. Upon the document's discovery in 2020, he immediately turned the document into the nearest SCIF that was located on a military installation. He provided full disclosure to the authorities when he surrendered the document. Several years have passed since this incident and it is unlikely to recur since Applicant no longer brings documents home.

AG ¶ 35(c) does not apply. While Applicant claims he was not fully trained before the 2007 incident, he admitted that he chose to eat the document because he did not want to drive back to work. His decision was made for his own personal convenience. I also considered that he did not disclose this incident until his 2018/2019 polygraph.

AG ¶ 35(d) partially applies to SOR ¶ 1.a because the violation was initially inadvertent and there appears to be no evidence of a compromise. It is unclear whether the faxed cover sheet was even classified. While he did not exercise the best judgment when he decided to eat the fax cover sheet, he destroyed the document. I cannot conclude he promptly reported the incident. He did not disclose this incident until a 2018/2019 polygraph interview.

AG ¶ 35(d) also applies to SOR ¶ 1.b. He inadvertently took home an e-mail which he labeled as Confidential. Upon the discovery of the e-mail, he promptly reported the incident, He immediately took the e-mail to a military installation that had a SCIF. The likelihood of compromise is low since the document was mixed in with a lot of unclassified documents that Applicant kept in his home.

While both of these incidents raise concerns, they were relatively minor and it is unlikely there was a compromise of classified information. Overall, Applicant mitigated the security concerns raised under Guideline K, Handling Protected Information.

**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 or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during the national security or adjudicative processes. . . .
>
> The following disqualifying conditions under AG ¶ 16 potentially apply:
>
> 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 individual may not properly safeguard classified or sensitive information. This includes, but is not limited to, consideration of: (3) a pattern of dishonesty or rule violations; and
>
> AG ¶ 16(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes: (1) Engaging in activities which, if known, could affect the person's personal, professional, or community standing.

With respect to SOR ¶ 2.a, "You failed to fully and timely report or disclose the conduct in subparagraphs 1.a and 1.b, as required.", and with respect to the allegation in SOR ¶ 1.a, both SOR ¶¶ 16(d) and 16(e) apply. The conduct alleged was the 2007 incident where Applicant discovered that he took home a classified cover sheet and ate the document rather than taking it back to the office. He failed to insure that he did not take home classified information, his decision to eat the classified fax cover sheet, and failure to report the incident to his chain of command and/or security officials raise questions about his trustworthiness, reliability and willingness to comply with rules and regulations. The concealment of this incident also created a vulnerability. Applicant's failure to promptly disclose the incident made him vulnerable to exploitation or manipulation.

I find for Applicant with respect to the second allegation in SOR ¶ 2.a, addressing SOR ¶ 1.b. When he discovered that he had inadvertently taken home an e-mail classified as Confidential, he immediately drove to a local military installation to turn it into a SCIF. He cooperated with the authorities at the military installation. I consider he timely and fully reported the incident alleged in SOR ¶ 1.b as soon as he discovered the issue.

Regarding SOR ¶ 2.b, regarding his termination from Employer A in April 2018, there is no record evidence that clearly explains the basis for Applicant's removal from the contract. Applicant testified he was never informed why he was removed from the contract. The evidence is insufficient to conclude that Applicant's termination from the project at the government customer's request raised a security concern. I note that the contractor attempted to place him on other contracts. They were unable to find another contract, so they had to let him go. I find for Applicant with respect to SOR ¶ 2.b.

Under Guideline E, the following mitigating conditions potentially apply:

> AG ¶ 17(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 is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
>
> AG ¶ 17(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that contributed to untrustworthy, unreliable, or other appropriate behavior, and such behavior is unlikely to recur; and
>
> AG ¶ 17(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

AG ¶ 17(c) applies with respect to SOR ¶ 2.a. It has been over 17 years, since Applicant ate the classified cover sheet and failed to report it to his supervisory chain. He fully disclosed the incident during a polygraph exam in 2018. The record remains unclear as to whether the cover sheet itself was actually classified. There were no classified markings on the cover sheet. There was a statement on the cover sheet that the cover sheet should be treated as classified information. While Applicant should have taken the more reasonable approach and returned the fax cover sheet to the office as well as disclosed the incident to his supervisor, his conduct is unlikely to recur.

AG ¶ 17(c) applies with respect to SOR ¶ 2.b. Applicant was terminated in April 2018 from Contractor A after the government customer requested he be removed from the project. There is nothing in the record that provides a basis for his removal. There is nothing in the record that shows this is related to him being a security risk. There is no evidence that government customer filed a security incident report. Since 2018 and 2019, Applicant has worked for numerous contractors. While he admits to being removed from five different government contracts, the record does not show the basis for these removals. The record evidence is lacking as to whether Applicant created a security concern when he was taken off these contracts. He could have been taken off the contracts due to other reasons such as insufficient work, personality conflicts, failure to fit in with the office culture, etc.

AG ¶ 17(d) applies. Applicant acknowledged that he did not report the 2007 incident involving the faxed cover sheet for classified information. Regarding the discovery of a confidential e-mail in 2020, Applicant immediately turned this document

into a local SCIF. Applicant's decision to take home a lot of unclassified documents for his personal files was the not the best judgment. He failed to insure that no classified documents were among the documents that he took home. He has since reviewed and destroyed the documents that he took home earlier in his career. He no longer takes unclassified documents home. He has taken steps to prevent these issues from happening again.

AG ¶ 17(e) applies because Applicant disclosed both minor security incidents. He has reduced his vulnerability to exploitation, manipulation, or duress.

**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.

At times in the past, Applicant has not demonstrated the best judgment in relation to handling classified and sensitive documents. However, his past security incidents were relatively minor. They do not appear to have compromised classified information. He no longer takes unclassified documents home. I found him to be forthcoming during the hearing. While he has been removed from government contracts at the request of the government customer on several occasions, the record evidence is unclear as to the basis for his removal from each contract. It is not unusual for employees to move often in contract positions.

I considered the potentially disqualifying and mitigating conditions as well as the facts and circumstances surrounding this case. The security concerns under Handling Protected Information and Personal Conduct 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 |
| Subparagraphs 1.a – 1.b: | For Applicant |
| Paragraph 2, Guideline E: | FOR APPLICANT |
| Subparagraphs 2.a – 2.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