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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| | ) | ISCR Case No. 18-01631 |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Nicole A. Smith, Esq., Department Counsel
For Applicant: Mark S. Zaid, Esq.
03/16/2020

_____

## Decision

_____

HEINTZELMAN, Caroline E., Administrative Judge:

Applicant mitigated the handling of protected information and use of information technology concerns. Based upon a review of the record as a whole, national security eligibility for access to classified information is granted.

## History of the Case

Applicant submitted a security clearance application (SCA) on April 4, 2014. On July 3, 2018, the Department of Defense (DOD) issued a Statement of Reasons (SOR) alleging security concerns under Guideline K (Handling Protected Information) and Guideline M (Use of Information Technology). Applicant answered the SOR on July 28, 2018, and requested a hearing before an administrative judge (Answer).

I was assigned to the case on December 4, 2018. On December 13, 2018, the Defense Office of Hearings and Appeals (DOHA) notified Applicant that the hearing was scheduled for January 9, 2019, and I issued an order to both parties to produce their documentary evidence by December 26, 2018. I convened the hearing as scheduled. Government Exhibits (GE) 1 was admitted. Applicant objected to the admissibility of GE 2, a polygraph examination report. I admitted it for limited purposes related to Applicant's statements made and not the polygraph test result. Any polygraph results described herein were included to show the processing of the security investigation and not for the

truth or accuracy of the polygraph results. Applicant Exhibits (AE) A through M were admitted without objection. Applicant and one witness testified. Hearing Exhibits (HE) I through IV were marked and made part of the record. I received the transcript (Tr.) on January 23, 2019, and the record closed.

## Findings of Fact

Applicant is 46 years old. He has been married to his wife since 1994, and they have two children, aged 10 and 19. He served on active duty in the U.S. Army from 1991 until 1995 when he was honorably discharged. Since 1996, he has worked as a defense contractor for various government agencies and has continuously held a security clearance. Applicant received a bachelor's degree in 2009. (Tr. 8-9, 55-57, 107-109; GE 1; AE A; AE B; AE C)

At the time of the hearing, Applicant worked for a large government department as a senior network engineer and held a top secret security clearance. Prior to his 2015 periodic reinvestigation, Appellant held a top secret sensitive compartmented information with polygraph security clearance (TS/SCI). He underwent polygraph examinations for two previous security clearance investigations. (Tr. 8-9, 103-104; GE 1; AE A)

The SOR alleged that between 2009 and 2015, Applicant hand drew diagrams of a classified system which contained classified internet protocol (IP) addresses and site locations and took them to his home. During this period, it is also alleged that Applicant improperly emailed a diagram containing classified IP addresses and site locations via an unclassified network. In his Answer and at the hearing, Applicant denied purposely or inadvertently bringing classified hand-drawn diagrams containing classified IP addresses and site locations to his home. Additionally, he denied intentionally and unintentionally emailing a diagram with classified IP addresses and site locations through an unclassified network. (Answer; Tr. 57-58, 96, 105; AE A)

In 2009, Applicant started working as a senior network engineer contractor at an agency within the DOD (Agency). At that time, Agency and its classified communication system (CCS) were undergoing a transition from a legacy network to a new architecture. CCS is the high-speed data, video, and voice network internet system for the intelligence community (IC) and Agency is the caretaker of the system. Applicant was chosen to facilitate the transition for some of the other, more established, engineers. In order to do this, he had to learn the old network and the new network, which took him about a year. Part of the integration process included reducing 4000 IP addresses to roughly 100, and there were no drawings of the old or new networks for the aggregation. Drawings and diagrams are used by network engineers to encourage stability, redundancy, and resiliency on the CCS network. At that time, Applicant also worked as the liaison between Agency and the IC agencies who used Agency's CCS. (Answer; Tr. 58-61; AE A)

At some point, Applicant started producing templates to facilitate the changes between the old and new networks. His supervisors approved him bringing unclassified work home to work on substantive issues. At no point did his supervisors express concern

about this behavior. AE I and AE J are examples of unclassified work Applicant brought to his home. (Answer; Tr. 62, 100-101; AE I; AE J)

On June 10, 2015, Applicant took his first of four polygraph examinations. The first exam was for the five-year periodic reinvestigation for his TS/SCI security clearance. He was admittedly nervous during the exam. Because the examiner determined that he had a significant response to questions about sabotage, a second exam was conducted on July 6, 2015. No opinion was provided regarding Applicant's response to questions regarding intentionally mishandling classified information. (Tr. 58, 62-65; GE 2)

According to the report, Applicant disclosed that he kept working papers at his home, and they depicted internet technology infrastructure, schematics, communication routes, and solutions for various defense and IC agencies. Applicant testified that he disagreed with the polygrapher's record of his statement, and he believed the examiner did not understand the scope of his work. At the hearing, he explained that he maintained classified and unclassified notebooks of his work. AE G and AE H are examples of work he kept in his unclassified notebook, and they were reviewed by Agency. According to Applicant, he tried to explain his work to the examiner and how he performed authorized outages, matured the network, and terraformed or touched every site in every region to prepare for the infrastructure. The classified diagrams were written in the classified notebook, which he always left at his worksite. Applicant did not intend to give the impression that he brought classified materials to his home. (Answer; Tr. 64-68, 70, 90-92, 98-99; GE 2)

At the conclusion of the second polygraph exam, the examiner referred the issues to the investigations division and insider threat program within Agency. As a result, Applicant's home was immediately searched by Agency. Applicant accompanied the Agency employees to his home and did not have access to his home between the interview and the search. At his home, he gave Agency employees access to his office, computer, and documents. Agency seized Applicant's personal computer, notebooks, and documents related to his work at Agency. He also gave Agency access to his personal email accounts and server. Two days after the search of his home, he voluntarily brought to Agency an additional hard drive that was missed during the search. In early September 2015, all of Applicant's belongings were returned to him. It was determined that none of his belongs contained classified information. Additionally, Applicant was unaware of Agency finding any classified information on his unclassified computer and email account. (Answer; Tr. 64-69, 71-76, 89-90, 93, 99-100, 102-103; GE 2; AE E; AE G; AE H)

On September 28, 2015, Applicant was polygraphed a third time. Sometime between the first examination in June 2015 and the third exam, he was required to take his annual training regarding the handling of classified information. The polygraph examination report indicated there were no opinions given regarding Applicant disclosing classified information. (Tr. 51-52, 68, 72, 75-76l; GE 2)

Two days later, Applicant was given a fourth and final polygraph examination. According to the examination report, the examiner had no opinions regarding Applicant's responses to questions regarding the handling of classified information. However, during the post-test session, the examiner noted that Applicant stated that he routinely made drawings of Agency's CCS, took them to his home, and plugged the information into a simulator for testing purposes. Between five and ten times, he failed to fully redact the IP addresses. Applicant testified that this information in the report is not accurate, and he did not intend to give the impression that the diagrams were classified, because they were not. (Tr. 76-77; GE 2)

During the post-test discussions following the fourth polygraph, Applicant disclosed that on one occasion in 2013, he inadvertently left a folder containing IP addresses and site locations on an Agency shuttle bus. The bus was used to transport employees from Agency's headquarters to a satellite location and to the employee parking lot. Several days later, he was able to find the folder on the bus, which remained in its zippered pouch. When he examined the papers in the folder he realized he failed to redact information. He was unsure if the information was classified, but it had the potential to be classified. He did not report this incident to his supervisor or to the appropriate authorities at Agency because the papers never left the Agency compound, and he believed the incident was minor. This is the one and only time that Applicant brought documentation that might be considered classified out of the office. He also admitted at the hearing that on four to five occasions, he may have failed to fully redact information, but the documents never left his secure work location. (Answer; Tr. 77-83, 93-98)

Applicant admitted at the hearing that the 2013 bus incident was potentially a security violation, but he has had no other security violations. If he were to inadvertently violate a security protocol in the future, Applicant would report it to his facility security officer and the appropriate government authorities. (Tr. 83, 105-106)

During one of the polygraph interviews, Applicant remembered that he sent an email to himself from his unclassified work account to his personal email that he thought might contain sensitive or classified information. While working at Agency, he worked on both unclassified and classified networks and computers. In response to the examiner's request, he produced the email. At the hearing, he explained that the email contained nothing sensitive or classified, which was confirmed in one of his letters of recommendation. (Tr. 87-90; AE F; AE L)

Following one of his polygraph interviews, Applicant was asked to sign a statement, which in part, indicated he had taken classified materials to his home. He refused to sign that statement as it was written. In October 2015, Applicant's SCI access was removed, and as a result, he could no longer work as a contractor for Agency. He was not given the opportunity to further explain or address Agency's concerns. (Tr. 49, 84-86; AE D)

Applicant's witness (Witness), a government team leader at Agency, has worked as an active duty military member and a federal employee since 1983. He previously

worked in computer engineering, but he has worked in network integration for over twenty years. Witness has held a TS/SCI with polygraph security clearance since 1987. (Tr. 37-39)

Witness and Applicant were coworkers between 2009 and 2015, when Applicant was removed from Agency. They interacted daily, and Witness was Applicant's team lead. Applicant and Witness were both engineers who were responsible for ensuring that CCS was operational and data and video was successfully transferred. (Tr. 39-41, 60-61)

Witness reviewed the SOR, GE 2, and AE F, and in his opinion Applicant did not violate classification protocol when he brought hand-drawn diagrams of the CCS system to his residence. The IP addresses alone were not classified, nor were the site locations, but when the two elements are combined, they become classified under mosaic rules and potential compromise results in a security incident. According to Witness, network engineers at Agency worked at their homes to enhance their mission by studying or practicing routing protocols on their home computer or their home network. They did this to run different scenarios. Applicant had a program at home in which he could run different scenarios on how to use different routing protocols. "On those protocols the only thing you need to do is input – you input IP addresses but you don't necessarily have to put your production or your classified IP addresses." (Tr. 42-46, 51, 53-54; AE F)

Witness was never aware of Applicant violating any security protocols. He had no concerns as to Applicant's suitability to hold a security clearance and to protect classified information. Applicant "had a great reputation with his coworkers and with management because of his tenacity in building the network." Witness described Applicant as honest, intelligent, compassionate, hardworking, loyal, and possessing high integrity. (Tr. 46-51)

Applicant's three letters of recommendation, were written by former and current co-workers. They all reviewed the SOR prior to submitting their letters and had no concerns as to Applicant's suitability to have access to classified information. They described Applicant as highly trustworthy, reliable, and knowledgeable. Despite the issuance of the SOR, he remained in Agency leadership's high esteem. (AE K; AE L; AE M)

Applicant's annual work appraisals from 2006 through December 2014, demonstrate that he consistently received positive reviews. During his years of military service, Applicant received an Army Achievement Medal and a Good Conduct Medal. He has also received multiple awards from his defense contractor employers, including his employer at the time of the hearing, and the government agencies he supported. (AE B; AE C)

## Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially

disqualifying conditions and mitigating conditions, which are to be used 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, administrative judges apply the guidelines 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(a), 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."

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 the applicant or proven by Department Counsel." The applicant has the ultimate burden of persuasion to obtain a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information. Section 7 of Exec. Or. 10865 provides that adverse 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* Exec. Or. 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

## Analysis

### 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 handling protected information-which includes classified and other sensitive government information, and proprietary 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 be disqualifying. The following are potentially applicable in this case:

> (b) collecting or storing protected information in any unauthorized location;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium; and
>
> (d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system.

According to the October 2015 Polygraph Report, Applicant admitted that he took materials, which in the aggregate or mosaic, contained classified information to his home. Additionally, on one occasion he sent an email to himself that also contained classified information.

Applicant at the hearing and in his Answer to the SOR, denied all of the underlying behavior that was alleged in the SOR. He testified that he did not tell the polygraph examiners that he violated security protocols other than the 2013 bus incident. Agency searched his home and seized his personal papers and computer. There was no evidence beyond the content of the polygraph report that Applicant possessed classified documents or information at his home or on his personal computer and network. Nor was there any corroborating evidence that he improperly (in violation of his supervisors' rules) emailed classified information from his classified and unclassified work email accounts and his personal email account. Additionally, it appears from the record evidence, that his habit of bringing unclassified work home or emailing unclassified components of his work to his personal email address was something his supervisors were aware of and encouraged.

The 2013 security incident was not alleged in the SOR and was not considered in determining if the disqualifying conditions applied. In this case, Applicant credibly testified regarding his habits, behavior, and mistakes he made. His failure to report the 2013 bus incident in a timely manner, is concerning; however, he did report the incident during his fourth polygraph examination and there is no evidence of compromise or a pattern of violations. The record evidence of a responsible, valued, and trustworthy employee substantially outweighs this mistake. Despite this incident and Applicant's subsequent failure to timely report his mistake, I am left without doubts as to Applicant's credibility, honesty, and trustworthiness. Applicant refuted the Guideline K disqualifying conditions.

**Guideline M: Use of Information Technology**

AG ¶ 39 expresses the security concern pertaining to use of information technology:

> Failure to comply 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 includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

AG ¶ 40 describes conditions that could raise a security concern and be disqualifying. The record evidence established that the following are applicable in this case:

> (d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system; and
>
> (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized.

The polygraph report provides sufficient evidence to raise AG ¶¶ 40(d) and 40(f). Applicant refuted the Guideline M disqualifying conditions for the reasons stated in the previous section.

**Whole-Person Concept**

Under AG ¶ 2(c), the ultimate determination of whether the granting or continuing of national security eligibility is clearly consistent with the interests of national security must be an overall common sense judgment based upon careful consideration of the pertinent guidelines, each of which is to be evaluated in the context of the whole person. An administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d):

> (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.

I have incorporated my comments under the guidelines at issue in my whole-person analysis, and I have considered the factors in AG ¶ 2(d). Applicant presented a strong whole-person case. The record evidence establishes Applicant is highly trustworthy, reliable, diligent, knowledgeable, and dedicated to mission accomplishment. After weighing the disqualifying and mitigating conditions under these guidelines, and evaluating all the evidence in the context of the whole person, Applicant refuted the security concerns at issue. The totality of the record evidence leaves me without doubts as to Applicant's suitability to hold a clearance. Accordingly, Applicant has carried his burden of showing that it is clearly consistent with the interests of national security of the United States to grant him eligibility for access to classified information.

## Formal Findings

I make the following formal findings on the allegations in the SOR:

| | |
|---|---|
| Paragraph 1, Guideline K: | FOR APPLICANT |
| Subparagraphs 1.a and 1.b: | For Applicant |
| Paragraph 2, Guideline M: | FOR APPLICANT |
| Subparagraph 2.a: | For Applicant |

## Conclusion

I conclude that it is clearly consistent with the national security interests of the United States to grant or continue Applicant's eligibility for access to classified information. National security eligibility is granted.

_____
Caroline E. Heintzelman
Administrative Judge