DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 17-01584
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Adrienne Driskill, Esq., Department Counsel
For Applicant: *Pro se*

06/25/2018

Decision

GOLDSTEIN, Jennifer I., Administrative Judge:

Applicant mitigated the concerns raised under the Handling Protected Information, Use of Information Technology, and Personal Conduct guidelines. Eligibility for access to classified information is granted.

Statement of the Case

On August 15, 2017, in accordance with DoD Directive 5220.6, as amended (Directive), the Department of Defense issued Applicant a Statement of Reasons (SOR) alleging facts that raise security concerns under the Handling Protected Information, Use of Information Technology, and Personal Conduct guidelines. The SOR further informed Applicant that, based on information available to the government, DoD adjudicators could not make the preliminary affirmative finding that it is clearly consistent with the national interest to grant or continue Applicant's security clearance.

Applicant answered the SOR on September 25, 2017, and requested a hearing before an administrative judge. (Answer.) The case was assigned to me on November 15, 2017. The Defense Office of Hearings and Appeals (DOHA) issued a notice of

hearing on December 13, 2017, scheduling the hearing for January 8, 2018. The hearing was convened as scheduled. The Government offered Exhibits (GE) 1 through 3, which were admitted without objection. Applicant testified on his own behalf. The record was left open until February 26, 2018, for receipt of additional documentation. On that date, he submitted Applicant's Exhibits (AE) A through D, which were admitted without objection. DOHA received the transcript of the hearing (Tr.) on February 5, 2018.

Findings of Fact

Applicant admitted the allegations in SOR ¶¶ 1.a, 2.a, and 3.a. After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is a 43-year-old employee of a defense contractor. He was employed by defense contractor 1 (DC-1) most recently from 2002 to February 27, 2015. He had previously worked for DC-1 in other capacities for brief periods of time. He has been employed with defense contractor 2 (DC-2) since March 2015. He held a security clearance from 2002 through 2015, while employed by DC-1, without incident. He is married, and has two sons, ages 12 and 14. (GE 1; Tr. 18-21.)

In 2015, Applicant accepted a job offer with DC-2 because his family wanted to relocate out of state. His new job with DC-2 was similar to the job duties he performed for DC-1. (Tr. 21-22.) He had left employment with DC-1 in the past, but always returned. He thought that he may return again in the future and wanted to store his work product so that he could pick up where he left off if he returned. As a result, he decided to make copies of his electronic work files. On February 19, 2015, he connected a personally-owned external hard drive, which could hold a terabyte of information, to his work computer. Company policy did not forbid the use of personally-owned external hard drives at that time. He selected the drive to copy, locked his computer screen, and then left for the night. He downloaded approximately 120,000 proprietary program files to his external hard drive over the course of the evening. He did not intend to use the files during his employment with DC-2. (GE 2; Tr. 32, 41-43.) He explained:

> I had a -- a hard drive laying around that I picked up on a Black Friday sale or something like that and -- and it was a large enough capacity to where I could just copy the entire network drive where I had stored all of my analysis over -- well, what I retained and saved of that analysis over the -- just about the entire time I had worked at [DC-1]. And it was, as you see by the evidence, a large number of files and it would have been just time-prohibitive to go through them all and cherry-pick need this one, this one, this one. So what I did is I just basically made a copy of the entire drive area. So it was mostly out of ease more than anything else. And that way, I would have everything backed up were I to return to that position. (Tr. 22-23.)

All of the files copied were on a drive in which Applicant was the administrator, and were files that Applicant worked on and generated while working for DC-1. Applicant admitted that the files copied contained DC-1 proprietary information. None of the files contained classified information. (GE 2; Tr. 26, 30-31.)

After leaving DC-1, Applicant did not access the hard drive. Shortly after starting employment with DC-2 he received a letter, dated March 6, 2015, from an attorney with DC-1. (GE 2; Tr. 49.) It stated:

> It has come to my attention that before the end of your employment with [DC-1], you downloaded and removed a large amount of [DC-1] data and information. I am writing to demand that you immediately return all [DC-1] data and information that you removed from [DC-1] systems or premises, whether via electronic media, hard copy, or other means. I also demand that you refrain from disclosing any [DC-1] data or information to any third party, take all actions necessary to protect the confidentiality of such data or information, and provide me with a written account of all of your unauthorized disclosures of [DC-1's] data and information.
>
> This is a very serious matter. Your actions may violate various state and federal laws governing the unauthorized access of proprietary computer systems, including the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030; the federal Electronic Communications Privacy Act, 18 U.S.C. § 2701; and the [state] Computer Crimes Law [citation omitted]. In addition, your actions likely violate the confidentiality agreement you signed when you were hired at [DC-1] and which you acknowledged in writing upon the termination of your employment. The confidentiality agreement legally obligates you not to use or disclose [DC-1] proprietary or confidential information that is not available to the general public. Your actions downloading and removing such information shortly before your employment ended seriously call into question whether you intended to comply with that agreement. (GE 3.)

When Applicant received this letter "the full weight of what [he] had done hit [him] immediately" and he called the attorney to "rectify the situation." (Tr. 36.) The attorney requested he return the hard drive to DC-1. He mailed it back the following Monday. (Tr. 36.) He fully complied with the letter. After mailing the hard drive to DC-1, he heard nothing further from DC-1. No legal actions were filed against him as a result of this incident. (Tr. 40-41, 50.) He is extremely remorseful and has gained a new appreciation for the protection of proprietary information.

Applicant informed his new manager and his security office at DC-2 of the letter from DC-1, and the circumstances that led to the letter. DC-2 has provided Applicant with briefings on company policy, computer security, security awareness, and the proper handling of protected materials. (AE B; AE C; AE D; Tr. 37.)

Policies

When evaluating an applicant's suitability for national security eligibility, the administrative judge must consider the pertinent AG. In addition to brief introductory explanations of the security concern, the guidelines list potentially disqualifying conditions and mitigating conditions, which are to be used in evaluating an applicant's national security eligibility.

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 AG ¶ 2 describing the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. The entire process is a conscientious scrutiny of applicable guidelines in the context 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. I have not drawn inferences based on mere speculation or conjecture.

Directive ¶ E3.1.14 requires the Government to present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "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, and has the ultimate burden of persuasion as to obtaining a favorable clearance decision."

A person applying for national security eligibility seeks to enter 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 national security eligibility. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified or sensitive information.

Finally, as emphasized in Section 7 of Executive Order 10865, "[a]ny determination under this order adverse to an applicant shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* Executive Order 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information.)

Analysis

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, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

The guideline notes several conditions that could raise security concerns under AG ¶ 34. Three are potentially applicable in this case:

> (d) inappropriate efforts to obtain or view protected information outside one's need to know;
>
> (f) viewing or downloading information from a secure system when the information is beyond the individual's need-to-know; and
>
> (g) any failure to comply with rules for the protection of classified or sensitive information.

Applicant downloaded files from the DC-1 computer system, in anticipation of leaving his employment there. He retained those files after he left DC-1, although he no longer had a need to access that information. His actions were in violation of company policies. The above disqualifying conditions apply.

AG ¶ 35 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 35 including:

> (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; and
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities.

As noted below under the discussion of the applicability of AG ¶ 41, Applicant was extremely remorseful. He has realized the gravity of his error and similar misconduct is unlikely to occur. He has responded favorably to training and

demonstrates a positive attitude about his security responsibilities. Applicant mitigated the concerns raised by the Handling Protected Information guideline.

Guideline M, Use of Information Technology

The security concern relating to the guideline for Use of Information Technology is set out in AG ¶ 39:

> 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.

The guideline notes several conditions that could raise security concerns under AG ¶ 40. One is potentially applicable in this case:

> (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.

In anticipation of Applicant's departure from DC-1, he duplicated proprietary files prior to leaving his employment. He violated the confidentiality agreement he signed when he was hired at DC-1, as well as other laws. AG ¶ 40(f) applies.

AG ¶ 41 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 41 including:

> (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;
>
> (b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness; and
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel.

Applicant's decision to copy company proprietary files was made in the interest of what he perceived to be organizational efficiency. He wanted to preserve the files in the

event of his possible return to employment there. He acknowledged that he made a grave misjudgment. He immediately returned the hard-drive to DC-1, when he realized the implications of his actions. No further actions were taken by DC-1. He has been fully forthcoming about his mistake, both with his current employer and during the security clearance process. Three years have now passed since that incident. He has completed additional training with his current employer. Similar events are unlikely to occur. The above conditions apply.

Guideline E, Personal Conduct

The security concern relating to the guideline for Financial Considerations 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 national security investigative or adjudicative processes. The following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation of further processing for national security eligibility:
>
> > (a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, cooperation with medical or psychological evaluation, or polygraph examination, if authorized and required; and
> >
> > (b) refusal to provide full, frank, and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

The guideline notes several conditions that could raise security concerns under AG ¶ 16. One is potentially applicable in this case:

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

As stated under the analysis for the preceding guidelines, Applicant violated his non-disclosure agreement by removing DC-1 proprietary materials when he left employment there. The evidence is sufficient to raise this disqualifying condition.

AG ¶ 17 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 17 including:

> (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;
>
> (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 inappropriate behavior, and such behavior is unlikely to recur; and
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

As discussed in detail above under Guidelines M and K, the above mitigating conditions apply.

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(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.

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 facts and circumstances surrounding this case. I have incorporated my comments under Guidelines K, M, and E in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines, but some warrant additional comment.

Applicant has an extended history of working in the defense industry. This was a one-time incident, and he is unlikely to commit further violations. Overall, the record

evidence leaves me without questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the Handling Protected Information, Use of Information Technology, and Personal Conduct security concerns.

Formal Findings

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

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

_____
Jennifer I. Goldstein
Administrative Judge