DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 12-01906
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Jeff A. Nagel, Department Counsel
For Applicant*: Pro se*

September 10, 2018

_____

Decision

_____

LOKEY ANDERSON, Darlene D., Administrative Judge:

Statement of the Case

On January 26, 2018, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline M, Use of Information Technology. 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) effective for cases after June 8, 2017.

Applicant answered the SOR on February 17, 2018, and requested a hearing before an administrative judge. The case was assigned to me on May 2, 2018. The Defense Office of Hearings and Appeals issued a notice of hearing on June 21, 2018, and the hearing was convened as scheduled on August 7, 2018. The Government offered four exhibits, referred to as Government Exhibits 1 through 4, which were admitted without objection. The Applicant offered four exhibits at the hearing, referred to as Applicant's Exhibits A through D. Applicant testified on his own behalf. The record

remained open until close of business on August 21, 2018, to allow the Applicant the opportunity to submit additional supporting documentation. Applicant submitted one Post-Hearing Exhibit, referred to as Applicant's Post-Hearing Exhibit A, which was admitted without objection. DOHA received the transcript of the hearing (Tr.) on August 15, 2018.

Findings of Fact

Applicant is 37 years old and married. He has a Master of Science degree in Engineering Management and Systems Engineering. He holds the position of Test Engineering Manager for a defense contractor. He seeks to obtain a security clearance in connection with his employment in the defense industry.

Paragraph 1 Guideline M – Use of Information Technology The Government alleges that the Applicant is ineligible for clearance because he has failed to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems, which raise security concerns about his ability to properly protect sensitive systems, network and information.

Applicant has worked in the defense industry since 2004. He received his first security clearance in 2004, while working for another defense contractor. As a result of a polygraph examination conduct in 2009, his security clearance was revoked. Applicant re-applied for a security clearance in 2014, which was granted.

Applicant worked for defense contractor A from February 2008 to October 2016. In 2016, while working for defense contractor A, without authorization and in contravention of his non-disclosure agreement, Applicant downloaded numerous files of company proprietary information on an encrypted thumb drive and took it with him after he had given notice of leaving the company. In November 2016, Applicant began working for defense contractor B, a competitor of defense contractor A. Applicant wanted to take the information on the thumb drive with him to the competitor where he was taking on a position of higher responsibility, as he knew that he would be working on the same engineering technology, and wanted to use it as a reference.

While at defense contractor A, he downloaded the information to an unsecured thumb drive. The thumb drive contained both company proprietary information as well as personal information. To further protect the information on the thumb drive, Applicant transferred the information on the thumb drive on to an ironkey, which is a more secure thumb drive. Applicant did this because if he went to work for another defense contractor, and he was working on the same program, although they were competitors in the industry, he could use the information to enhance his situation. The information transferred included cost pricing data and export control materials among other technology owned by contractor A. Applicant did not get permission to transfer this company proprietary information, nor was he authorized to do so. He states that he had no intention to share it with anybody, but that it was for his personal use. Applicant states that he was not aware of the severity of this actions until he received a letter from

the FBI and from his previous employer. Applicant also had a covenant not to compete precluding him from taking any technology he developed for Company A to another company. An internal investigation was conducted, and it was determined that Applicant violated company rules and regulations, and committed a security violation.

Applicant claims that he made an honest, naive, and very foolish mistake when he left company A, and that he really did not understand ramifications of his actions. (See Tr. p. 14, and Applicant's Answer to SOR.)

Letters for recommendation from his operations manager, recruiter, an administrative assistant, and other engineers with whom he works, state that Applicant is trustworthy and responsible and they would like to see his security clearance reinstated. (Applicant's Exhibit B.)

A letter from the Applicant's counselor with whom Applicant sought out a year of individual psychotherapy related to the loss of his security clearance in 2009, indicates that he would never knowingly damage any aspect an employer's privileged information. (Applicant's Exhibit A.)

Letters from his priest and two others working in the ministry, indicates that Applicant is highly professional and trustworthy. He is well-liked by the congregation, demonstrates good character, is always respectful, and has an ability to motivate others. (Applicant's Exhibit C.)

Applicant submitted a chart showing that Applicant's security clearance was reinstated in 2014. (Applicant's Exhibit D.)

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 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(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 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 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 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 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* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline M, Use of Information Technology

The security concern for Use of Information Technology is set out in AG ¶ 39, as follows:

> 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. Three are potentially applicable in this case:

(d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;

(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; and

(g) negligence or lax security practices in handling information technology that persists despite counseling by management.

Applicant without authorization and in contravention of his non-disclosure agreement wrongfully downloaded numerous company proprietary files. Applicant knew or should have known that this intentional conduct shows poor judgment, unreliability and untrustworthiness. Applicant committed a serious security violation. The evidence is sufficient to raise the above disqualifying conditions.

Four Use of Technology Mitigating Conditions under AG ¶ 41 are potentially applicable:

(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;

(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; and

(d) the misuse was due to improper or inadequate training or unclear instructions.

None of the mitigating conditions are applicable here. Applicant deliberately downloaded the proprietary information to the thumb drive and then to the ironkey without permission for the direct purpose of benefitting himself at his new company. He knew or should have known that this conduct was against company rules and regulations and against his non-disclosure agreement. Furthermore, he has a history of negligence and misconduct. His security clearance was first revoked in 2009. In 2014, Applicant, made some very improper decisions that have now negatively impacted his current clearance. Under the circumstances, Applicant's conduct in totality is outrageous, and unacceptable for a man of his caliber and education. He has not demonstrated that he is reasonable, responsible, or trustworthy or that his decision making shows good judgment as it would relate to his Use of Information Technology.

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 the facts and circumstances surrounding this case. I have incorporated my comments under Guideline M in my whole-person analysis. Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the Use of Information Technology security concerns.

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 M:	AGAINST APPLICANT
Subparagraph 1.a.:	Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant Applicant national security eligibility for a security clearance. Eligibility for access to classified information is denied.

Darlene Lokey Anderson
Administrative Judge