DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 18-01831
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Aubrey De Angelis, Esq., Department Counsel
For Applicant: *Pro se*

11/13/2019

_____

Decision

_____

NOEL, Nichole L., Administrative Judge:

Applicant contests the Defense Department's intent to revoke her eligibility for access to classified information. She did not provide sufficient evidence to mitigate the security concerns raised by her failure to comply with her employer's rules for handling proprietary information. Clearance is denied.

Statement of the Case

The Department of Defense Consolidated Adjudication Facility (DOD CAF) issued a Statement of Reasons (SOR) detailing security concerns under the handling protected information guideline on August 27, 2018. The DOD CAF took this action under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry*, signed by President Eisenhower on February 20, 1960, as amended; as well as DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program*, dated January 2, 1992, as amended (Directive), and the *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, implemented on June 8, 2017. Based on the available information, DOD adjudicators were unable to find that it is clearly consistent with the national interest to grant Applicant's security clearance and recommended that the case be submitted to an administrative judge for a determination whether to revoke or deny Applicant's security clearance.

Applicant answered the SOR on September 26, 2018, and requested a decision without a hearing. The Government submitted its written case on April 22, 2019. A complete copy of the file of relevant material (FORM) and the Directive were provided to Applicant. She received the FORM on May 8, 2019, and provided a response. The attachments to the FORM are admitted to the record as Government's Exhibits (GE) 1 through 8, and Applicant's response to the FORM is admitted as Applicant's Exhibit (AE) A through E, without objection.

Findings of Fact

Applicant, 55, has worked for her employer (Company A), a federal contracting company since 1991. She was granted access to classified information in 2004. Her eligibility was renewed after a 2014 periodic reinvestigation. In September 2017, Applicant's employer filed an incident report in the Joint Personnel Adjudication System (JPAS), alerting the DOD CAF that Applicant mishandled Company A proprietary information. This incident is the basis of the SOR.

After receiving an allegation of misconduct against Applicant, Company A began an investigation into her use of their IT system. The investigation determined that between December 2016 and September 2017, Applicant downloaded over 150,000 files onto five personal storage devices. The investigation established that Applicant was up to date on Company A training regarding the handling and storage of proprietary information. The investigation also established that Applicant acted in knowing violation of company policy.

An audit of Applicant's activity showed that she initiated at least 23 copy events from the Company A network between December 2016 and September 2017. She admits downloading an unspecified number of files in December 2016, so that she could continue to work during her end-of-year break when the Company A network would not be available to her. In April 2017, Applicant learned that she would be laid off from her position in Group 1 within the following 60 days. In May 2017, Applicant initiated 14 download events, copying over 59,000 files onto personal storage devices. She claims that she need the files to help her colleagues in Group 1 as needed. She also claims that she began working for Group 2 on a temporary basis in May 2017.

Applicant considered her transition from Group 1 to Group 2 difficult; as it required her to surrender the computers she used in her Group 1 position and obtain new computers for her position in Group 2. Transferring the files she needed between her old and new computers in accordance with Company A policy was also time consuming. In the interest of convenience, Applicant decided to download the files she needed to personal storage devices. She did not want to trouble her new supervisor in Group 2 with the details of the file transfers. She was more focused on impressing him with her performance during her probationary period. Although the investigation determined that Applicant continued downloading proprietary information until September 2017, it does not specify the number of files she downloaded between June and September 2017, or Applicant's reasons for doing so.

During the investigation, Company A interviewed Applicant's Group 1 and Group 2 supervisors and had them review the list of the files Applicant downloaded. Neither could identify a legitimate reason for Applicant to have possession of the downloaded files. According to Applicant's Group 2 supervisor, Applicant did not join the group until June 2017. Her position was not related to the position she previously held in Group 1 and did not require the use of any data from Group 1. According to Applicant's Group 1 supervisor, Applicant was not expected to continue working on Group 1 projects after she began her position in Group 2.

Applicant returned four of the five storage devices containing the downloaded files to Company A in September 2017. She could not find the fifth device, but promised to surrender if she was able to find it. She claims that she did not disclose the data to anyone outside Company A. Ultimately, the investigation concluded that Applicant did not adhere to the expected behavior of Company A employees when she copied Company A proprietary information on external storage devices. She received a warning letter reminding her of her obligation to protect Company A proprietary information and to adhere to Company A policies regarding the handling and protecting proprietary information. She was warned that another violation could result in correction action, up to and including discharge from Company A.

Character letters from Applicant's current Group 2 supervisor and other longtime coworkers describe her as trustworthy. They ascribe Applicant's actions to a misunderstanding of Company A policy.

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." 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 safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information.

Analysis

The record establishes that Applicant engaged in disqualifying conduct under the handling protected information guideline. An investigation by Applicant's employer determined she failed to comply with rules and regulations for handling the company's proprietary information, which raises doubt about her ability to handle and protect sensitive and classified information as well as her ability to follow rules and regulations. Her misconduct also highlights concerns about her judgment, trustworthiness and reliability. (See AG ¶ 33). Applicant violated her company's polices regarding the handling of proprietary information by intentionally downloading and saving over 150,000 files on five personal storage devices between December 2016 and September 2017. (AG ¶¶ 34(b) and (c)).

Although Applicant's actions did not result in the compromise of her employer's proprietary information, her actions continue to reflect negatively on her ongoing security worthiness. Her actions were not the result of improper or inadequate training, but intentional conduct meant to circumvent her employer's procedures, which she deemed time consuming and inconvenient. Furthermore, she failed to maintain physical security of the storage devices. Applicant's conduct also raises significant credibility issues. Despite her claims to the contrary, Applicant had no legitimate reason to store Company A proprietary data to personal storage devices. She had no official need for access to the downloaded files outside of duty hours or times when the Company A network would be unavailable to her. She had no need to maintain access to the downloaded files during her transition from Group 1 to Group 2 or thereafter. While it does not appear that Applicant's actions were motivated by malice against her employer, her actions show that she is willing to put her self interests above those of her employer's need to protect proprietary information. Accordingly, none of the relevant mitigating conditions apply.

Based on the record, doubts remain about Applicant's reliability, trustworthiness, good judgment, and ability to protect classified or sensitive information. In reaching this

conclusion, I have also considered the whole-person factors enumerated in AG ¶ 2(d). Applicant has worked for Company A for 23 years and has held a security clearance for at least 15 years. Although Applicant's employer treated her actions as an isolated incident of minor misconduct, the government is not obliged to do the same. Applicant is not entitled to retain her security clearance and the government is not required to wait until she actually mishandles classified information before deciding to revoke her access to classified information. The purpose of the security clearance adjudication is to make "an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk." (AG ¶ 2(d)). Applicant demonstrated a willingness to disregard her employer's rules related to the handling and safeguarding proprietary information. In doing so, she displayed poor judgment, lack of trustworthiness and reliability that create an unacceptable security risk.

Formal Findings

The formal findings on the SOR allegations are:

Paragraph 1, Guideline K:	Against Applicant
Subparagraph 1.a:	Against Applicant

Conclusion

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

Nichole L. Noel
Administrative Judge