DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	
[NAME REDACTED]	)	ISCR Case No. 20-00306
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Allison Marie, Esq., Department Counsel
For Applicant: *Pro se*

08/05/2021

_____

Decision

_____

MALONE, Matthew E., Administrative Judge:

Applicant did not mitigate the security concerns raised by her failure to protect sensitive information and by her lack of candor during an investigation into that conduct. Her request for eligibility for continued access to classified information is denied.

Statement of the Case

On October 23, 2017, Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) to renew her eligibility for access to classified information as part of her employment with a defense contractor. After reviewing the completed background investigation, adjudicators for the Department of Defense (DOD) could not determine that it was clearly consistent with the interests of national security for Applicant to have access to classified information, as required by Executive Order 10865, as amended, and by DOD Directive 5220.6 (Directive).

On December 2, 2020, the Defense Counterintelligence and Security Agency (DCSA) issued a Statement of Reasons (SOR) alleging facts and security concerns addressed under Guideline K (Handling Protected Information) and Guideline E (Personal Conduct). The adjudicative guidelines (AG) cited in the SOR were issued by the Director of National Intelligence (DNI) on December 10, 2016, to be effective for all adjudicative actions taken on or after June 8, 2017. Applicant responded to the SOR (Answer) on January 20, 2021, and requested a decision without a hearing.

On March 31, 2021, as provided for by paragraph E3.1.7 of the Directive, Department Counsel for the Defense Office of Hearings and Appeals (DOHA) issued a File of Relevant Material (FORM) that was received by Applicant on April 6, 2021. The FORM contained eight exhibits (Items 1 – 8) on which the Government relies to support the SOR allegations. Applicant was informed she had 30 days from receipt of the FORM to submit additional information. During that time, Applicant did not submit additional information or object to the admission of any of the Government's documents into the record. The record closed on May 6, 2021, and I received the case for decision on July 20, 2021.

Findings of Fact

Under Guideline K, the SOR alleged that in October 2015, Applicant emailed 37 documents containing sensitive information from her work email to her personal email accounts; that she was suspended during her employer's investigation of her conduct; and that in November 2015, she was fired as a result of her actions (SOR 1.a). (FORM, Item 1)

Under Guideline E, the SOR cross-alleged the information in SOR 1.a (SOR 2.a). It was further alleged that during her employer's investigation into her actions, Applicant intentionally made false statements in an attempt to minimize the true scope of her misconduct (SOR 2.b). (FORM, Item 1)

In response to the SOR, Applicant admitted, with explanations, all of the allegations. (FORM, Item 3) In addition to the facts established by Applicant's admissions, I make the following findings of fact.

Applicant is a 56-year-old senior software engineer employed by a defense contractor in a position that requires a security clearance. In December 1987, she graduated from college with a Bachelor of Science degree in electrical engineering. Applicant and her husband have been married since August 1990 and have three children, all now in their 20s. She has worked for her current employer (Company A) since December 2015. Applicant previously worked as a senior systems engineer for a different defense contractor (Company B) between March and November 2015. Between August 2013 and March 2015, Applicant worked as a software engineer for two companies not involved in the defense industry. She first received a security clearance in 2008 in connection with her employment as a senior software engineer at a defense contractor between May 2007 and April 2013. (FORM, Items 4 and 5)

In e-QIP Section 13A (*Employment Activities*), Applicant disclosed that she had left her job with Company A "by mutual agreement" due to "misconduct." During the ensuing background investigation, information was obtained that showed Applicant had intentionally sent documents containing sensitive information to her personal email accounts. Even though the documents were not classified, most were proprietary documents containing sensitive information about Company B's development of systems for its federal government customer. As such, company policy required that employees protect those documents from unauthorized disclosure. Applicant was not authorized to transmit the documents in question outside the control of Company B information systems. Available information further shows that Applicant actually was fired from her Company B position rather than leaving "by mutual agreement." (FORM, Items 3, 4, 5, and 7)

On October 14, 2015, Applicant was interviewed by Company B security officials, who asked Applicant if she had sent sensitive or proprietary information to her personal email. At first, Applicant was evasive about her actions, admitting to sending one document. She then stated she sent "a few" documents, then "five" documents. At that time, after giving consent to search her Company B computer and employee email account, Applicant was suspended pending completion of Company B's investigation. Ultimately, 37 documents were identified as having been transmitted between April and October 2015 to four personal email accounts attributed to Applicant. She has claimed that she was not truthful when interviewed because she felt intimidated by Company B officials. In response to SOR Guideline E allegations, Applicant claims she was under duress during the Company B interview. (FORM, Items 3, 5, and 7)

Concurrent with Company B's investigation, the FBI also investigated Applicant's actions as possible economic espionage. The investigation lasted from October 2015 until January 2016, closing after the Department of Justice declined prosecution. During an interview with FBI agents on January 7, 2016, Applicant confirmed that she had deleted from her email accounts, computer, and handheld devices, all of the files she had sent. The FBI report of investigation further shows that Applicant was not truthful in October 2015, when she was first interviewed by Company B officials. In her response to the SOR, Applicant claimed that the FBI agents informed her that Company B "did not handle this incident correctly, and has blown this incident out of proportion." Nothing in the FBI report or any other portion of this record supports her claim. (FORM, Items 5 and 8)

On April 25, 2019, Applicant was interviewed by a government investigator as part of her background investigation. During that interview, Applicant stated that she did not understand that the information she emailed to herself needed to be protected in much the same way as information that was actually classified. Further, and as she also stated in response to the SOR, Applicant averred that she had not received adequate training regarding protection of sensitive information. Finally, Applicant characterized her actions in sending 37 documents to her personal email accounts as "inadvertent." (FORM, Items 3 and 5)

On March 3, 2015, when she first began working at Company B, Applicant executed a "Confidentiality and Innovation Agreement" whereby she agreed that the

information for which she might be responsible during her employment was sensitive, proprietary information, the unauthorized disclosure of which would be contrary to internal company policies and, potentially, the Economic Espionage Act of 1996. At the outset of her employment with Company B, Applicant also completed extensive training in matters related to the protection of classified information as well as other sensitive and proprietary information. In response to the SOR, Applicant claims there has been no recurrence of this type of conduct since 2015. She further avers that Company A, for whom she now works, has given her the training and resources she needs to perform her duties without mishandling sensitive information. Applicant produced information that shows she has received numerous awards for her work at Company A; however, she did not provide any information that would corroborate her claims regarding training and resources. (FORM, Items 3, 6, and 7)

Policies

Each security clearance decision must be a fair, impartial, and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the adjudicative guidelines (AG). (*See* Directive, 6.3) Decisions must also reflect consideration of the factors listed in AG ¶ 2(d). Commonly referred to as the "whole-person" concept, those factors are:

> (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.

The presence or absence of a disqualifying or mitigating condition is not determinative of a conclusion for or against an applicant. However, specific applicable guidelines should be followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified information. A security clearance decision is intended only to resolve whether it is clearly consistent with the national interest for an applicant to either receive or continue to have access to classified information. (Department of the Navy v. Egan, 484 U.S. 518 (1988))

The Government bears the initial burden of producing admissible information on which it based the preliminary decision to deny or revoke a security clearance for an applicant. Additionally, the Government must be able to prove controverted facts alleged in the SOR. If the Government meets its burden, it then falls to the applicant to refute, extenuate or mitigate the Government's case. Because no one has a "right" to a security clearance, an applicant bears a heavy burden of persuasion. (*See* Egan, 484 U.S. at 528, 531) A person who has access to classified information enters into a fiduciary relationship with the Government based on trust and confidence. Thus, the Government has a

compelling interest in ensuring each applicant possesses the requisite judgment, reliability and trustworthiness of one who will protect the national interests as his or her own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the Government. (*See* Egan; AG ¶ 2(b))

Analysis

Guideline K: Handling Protected Information

Available information about Applicant's mishandling of sensitive information while employed at Company B reasonably raises a security concern about her willingness and ability to properly handle protected information. That concern is stated at 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 doubts about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

Between March and October 2015, Applicant knowingly transferred to her four personal email accounts at least 37 documents containing information her employer deemed as proprietary and sensitive to Company B's work in support of the federal government. This information establishes the following AG ¶ 34 disqualifying conditions:

> (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
>
> (g) any failure to comply with rules for the protection of classified or sensitive information.

By contrast, Applicant has claimed that her actions were inadvertent, and that Company B did not provide her with the proper training and resources as she claims has been the case at Company A. Additionally, Applicant cites the passage of nearly six years without a recurrence of her actions at Company B. These claims require consideration of the following AG ¶ 35 mitigating conditions:

> (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;

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

(c) the security violations were due to improper or inadequate training or unclear instructions; and

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

All available information probative of these mitigating conditions leads me to conclude that none apply here. As to AG ¶¶ 35(a), 35(c) and 35(d), although six years have elapsed without a recurrence of the events cited in the SOR, Applicant's mischaracterization in her e-QIP of the circumstances of her job termination and her continued false claims that her conduct was "inadvertent" undermine confidence in her judgment and reliability. It is beyond question that Applicant was fired and did not leave Company B by mutual agreement. It is also beyond question that her actions were deliberate and multiple. As to training, Applicant's conduct occurred over the seven months after she signed a "Confidentiality and Innovation Agreement," and after she received extensive training in the protection of sensitive information when she began her employment with Company B in March 2015. It is reasonable to conclude that she was adequately trained in procedures to protect sensitive and proprietary information, and that she knew the information she emailed to herself was subject to those procedures.

Applicant also is unable to benefit from application of AG ¶ 35(b). She claims that her current employer, Company A, has provided her with better training and resources with which to do her job while protecting information as required. However, Applicant did not provide any information about that training, or about her adherence to security procedures, from which to conclude that AG ¶ 35(b) can be applied. On balance, Applicant failed to present information sufficient to mitigate the security concerns under this guideline.

Guideline E: Personal Conduct

Available information shows that Applicant knowingly made false statements to Company B officials when she was interviewed in March 2015. This information, as well as information about her mishandling of protected information, reasonably raises the security concerns addressed at 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.

More specifically, the Government's information establishes the following AG ¶ 16 disqualifying conditions:

(b) deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative; and

(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: (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or government protected information.

I also have considered the following AG ¶ 17 mitigating conditions:

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

(b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by advice of legal counsel or of a person with professional responsibilities for advising or instructing the individual specifically concerning security processes. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;

(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; and

(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.

As to AG ¶¶ 17(a) and 17(b), the record shows that when she was interviewed by Company B officials, Applicant attempted to grossly minimize the actual scope of her misconduct. It was not until she was suspended from work and those officials were able to search her company computer and email account that all 37 documents were identified. Additionally, Applicant was not being advised in her answers by anyone authorized to do so. Finally, she has never herself corrected the misrepresentations she made during the interview. AG ¶¶ 17(a) and 17(b) do not apply.

AG ¶¶ 17(c) and 17(d) do not apply for the same reasons AG ¶¶ 35(a) – 35(d) do not apply. Applicant continues to characterize her disclosures as inadvertent and as the product of insufficient training. She also did not support her claims regarding recent training (the equivalent of "counseling" in AG ¶ 17(d)) that might preclude a recurrence of her misconduct. On this issue, I have considered the fact that she falsified the nature of her Company B termination in her most recent e-QIP. She also insisted on characterizing her conduct as inadvertent, both in response to the SOR and during her subject interview in 2019. Although not alleged in the SOR, this information is relevant to an assessment of her current credibility and rehabilitation. Applicant did not mitigate the security concerns under this guideline.

In addition to my evaluation of the facts and application of the appropriate adjudicative factors under Guidelines E and K, I have reviewed the record before me in the context of the whole-person factors listed in AG ¶ 2(d). Applicant received several awards for her work with Company A; however, she did not present necessary information about her training and about her adherence to procedures for protection of sensitive information. Additionally, she made statements in response to the Government's information that continue to cast doubt on her judgement and trustworthiness. Accordingly, available information is not sufficient to resolve the doubts about Applicant's suitability for a security clearance that have been raised by the Government's case. Because protection of the national interest is the principal focus in these adjudications, any remaining doubts must be resolved against allowing access to sensitive information.

Formal Findings

Formal findings 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:	AGAINST APPLICANT
Subparagraphs 1.a:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraphs 2.a – 2.b:	Against Applicant

Conclusion

In light of all available information, it is not clearly consistent with the interests of national security for Applicant to have access to classified information. Applicant's request for security clearance eligibility is denied.

MATTHEW E. MALONE
Administrative Judge