DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 17-03051
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Mary M. Foreman, Esq., Department Counsel
For Applicant: *Pro se*

02/15/2019

_____

Decision

_____

CERVI, Gregg A., Administrative Judge

This case involves security concerns raised under Guidelines E (Personal Conduct), K (Handling Protected Information), and M (Use of Information Technology). Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on November 11, 2014. On November 27, 2017, the Department of Defense Consolidated Adjudications Facility (DOD CAF) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines E, K, and M.[1]

Applicant responded to the SOR on December 15, 2017, and requested a hearing before an administrative judge. The case was assigned to me on June 18, 2018. The

[1] The DOD CAF acted under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective on June 8, 2017.

Defense Office of Hearings and Appeals issued a notice of hearing on August 1, 2018, and the hearing was convened on August 29, 2018. Government Exhibits (GE) 1 through 4 were admitted into evidence without objection. Applicant testified at the hearing, but did not introduce any documentary evidence. DOHA received the hearing transcript (Tr.) on September 7, 2018.

Findings of Fact

Applicant is a 63-year-old contracts manager for a defense contractor, employed since 2014. He previously worked for another defense contractor from 2009 until he was laid off in 2013. Applicant received a bachelor's degree in 1980. He married in 1982 and has two adult children. He held a DOD security clearance for 30 years before he was laid off in 2013.

The SOR alleges under Guideline E that Applicant copied company proprietary files after being notified that he was selected for layoff. When confronted, he denied having the files, until he admitted copying them after repeated questioning. Applicant also falsified material facts presented to a Government investigator regarding this incident. The incident described in SOR ¶ 1.a is cross-alleged under Guidelines K and M. In his Answer to the SOR, Applicant denied intentionally copying the 661 files, and that it was not his intent to do so. Rather, he intended to copy examples of his work for use in finding another job, as he was in a "panic mode." He noted that he had permission to work from home and that the Government investigator was "misleading." The Government's evidence is sufficient to establish the SOR allegations.

On August 1, 2013, Applicant was notified that he was selected for layoff. He was notified not to have contact with company customers during the transition. The company began to monitor his work computer. Subsequently, Applicant removed three boxes from the office and composed an email to the contracts team and copied the customer. On Sunday, August 4, 2013, Applicant accessed the company computer system remotely, deleted certain data and copied 661 files to his personal thumb drive. The files were contract related information, including sensitive company financial information and proprietary information including contracts, contract negotiation information, and attorney work-product.

On August 8, 2013, Applicant met with company human resources and security personnel. He signed several statements affirming that he was not in possession of company proprietary information and electronic media. He was asked three times if he had any company data in his possession, and Applicant denied it each time. The fourth time, he admitted he may have information he copied for the transition. When the list of 661 files was presented to him, he admitted he had copied the files for "reference" purposes. He returned the thumb drive as directed.

When interviewed by a Government investigator in 2015, Applicant claimed he copied files with his supervisor's permission over a period of time to a company thumb drive and he was unaware of making any false statements to company personnel.

In Applicant's Answer to the SOR, he generally denied any wrongdoing with regard to copying documents, and claimed the Government investigator was "misleading." He stated that he was focused on getting his job done, and when he lost use of a company issued thumb drive, he used his personal thumb drive, and he did not remember that until he was confronted with specifics. He apologized for his actions and stated that "what I did after I lost my job was really stupid, and the only excuse I can offer is my state of mind at the time."

During the hearing in this case, Applicant admitted that he did things he should not have, including taking company documents that were useful to his new job and was deceptive to the company. However, Applicant also testified that the he did not take files for an improper purpose and denied having company proprietary information. When questioned, he admitted having company foreign contracts and attorney-client information. He also stated that he forgot the thumb drive was in his possession when confronted by the company, and claimed that he copied documents routinely as part of his work, but could not remember if he had a company laptop or a way to connect to the company computer system when away from work. He has not sought counseling to address this issue.

Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to "control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id.* at 527. The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865 § 2.

National security eligibility is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies these guidelines in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider a person's stability, trustworthiness, reliability, discretion, character, honesty, and judgment. AG ¶ 1(b).

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information.

Clearance decisions must be made "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See, e.g.,* ISCR Case No. 12-01295 at 3 (App. Bd. Jan. 20, 2015).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. *See, e.g.,* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see,* AG ¶ 1(d).

Analysis

Guideline E; Personal Conduct

AG ¶ 15 expresses the personal conduct security concern:

> 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.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying in this case. The following disqualifying condition are potentially applicable:

> (a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications,

award benefits or status, determine national security eligibility or trustworthiness, or award fiduciary responsibilities;

(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;

(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 person may not properly safeguard protected 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 other government protected information . . .;
>
> (4) evidence of significant misuse of Government or other employer's time or resources; and

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes:

> (1) engaging in activities which, if known, could affect the person's personal, professional, or community standing;

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying in this case. The personal conduct alleged is generally sufficient to implicate AG ¶¶ 16 (a), (b), (d), and (e).

Guideline E includes conditions that could mitigate security concerns arising from personal conduct. I have considered all of the mitigating conditions under AG ¶ 17 and found that none are fully applicable in this case.

I find that Applicant willfully copied 661 company documents without permission, and repeatedly lied to his employer before returning them. He also lied and was vague when answering questions related to this incident when interviewed by a Government investigator and when testifying at his hearing in this case. Applicant has not fully

apologized, but he continues to equivocate about his intent and the substance of the copied documents. He intentionally failed to cooperate when confronted by the company or Government investigator, and gave false and evasive answers. He has not sought counseling. Based on Applicant's significant loss of judgment, secretive nature of his actions, and failure to admit his possession of the files, even after being confronted, affirms his questionable judgment, lack of candor, dishonesty and unwillingness to comply with rules and regulations. I am not convinced that this incident is behind him or that similar intentional conduct will not recur. No mitigation fully applies.

Guideline K: Handling Protected Information

AG ¶ 33 expresses the handling protected information security concern:

> 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.

Relevant conditions that could raise a security concern under AG ¶ 34 and may be disqualifying include:

> (a) deliberate or negligent disclosure of protected information to unauthorized persons, including, but not limited to, personal or business contacts, the media, or persons present at seminars, meetings, or conferences;
>
> (b) collecting or storing protected information in any unauthorized location;
>
> (c) loading, drafting, editing, 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.

The evidence presented is sufficient to raise the security concerns described above.

Guideline K includes conditions that could mitigate security concerns arising from incidents regarding handling protected information. I have considered all of the mitigating conditions under AG ¶ 35. The findings of fact, discussion and reasoning under Guideline E, above, apply equally to the concerns raised under Guideline K, and are incorporated herein. I find no mitigating condition under Guideline K is fully applicable to Applicant's conduct.

Guideline M: Use of Information Technology Systems

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

> 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.

Relevant conditions that could raise a security concern under AG ¶ 40 and may be disqualifying include:

> (d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;
>
> (e) unauthorized use of any 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 evidence presented is sufficient to raise the security concerns described above.

Guideline M includes conditions that could mitigate security concerns arising from incidents regarding use of information technology. I have considered all of the mitigating conditions under AG ¶ 35. The findings of fact, discussion and reasoning under Guideline E, above, apply equally to the concerns raised under Guideline M, and are incorporated herein. I find no mitigating condition under Guideline M is fully applicable to Applicant's conduct.

Whole-Person Concept

Under AG ¶¶ 2(a), 2(c), and 2(d), the ultimate determination of whether to grant national security eligibility must be an overall commonsense judgment based upon careful consideration of the guidelines and the 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).

I considered all of the potentially disqualifying and mitigating conditions in light of the facts and circumstances surrounding this case. I have incorporated my findings of fact and comments under Guidelines E, K, and M, in my whole-person analysis. I also considered Applicant's long history of employment and security eligibility. However, his intentional actions to copy protected information for his personal use in another position, falsifying his actions when confronted, and falsifying and equivocating his involvement to a Government investigator and in his hearing, shows a complete lack of judgment, honesty, and trustworthiness expected of a person entrusted with national security eligibility. I remain unconvinced that this incident is behind him and will not recur.

Accordingly, I conclude Applicant has not carried his burden of showing that it is clearly consistent with the national security interests of the United States to grant him eligibility for access to classified information.

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 E:	AGAINST APPLICANT
Subparagraphs 1.a and 1.b:	Against Applicant
Paragraph 2, Guideline K:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline M:	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant

Conclusion

I conclude that it is not clearly consistent with the national security interests of the United States to grant Applicant's eligibility for access to classified information. Applicant's security clearance is denied.

_____
Gregg A. Cervi
Administrative Judge