DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 17-03757
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Andrew Henderson, Department Counsel
For Applicant*: Pro se*

October 26, 2018

_____

Decision

_____

LOKEY ANDERSON, Darlene D., Administrative Judge:

Statement of the Case

Applicant submitted his Electronic Questionnaire for Investigative Processing (e-OIP) dated November 2, 2016. (Government Exhibit 1.) On May 9, 2018, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline K, Handling Protected Information; Guideline M, Use of Information Technology; and Guideline E, Personal Conduct. 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 May 22, 2018, and requested a hearing before an administrative judge. The case was assigned to me on August 27, 2018. The Defense Office of Hearings and Appeals issued a notice of hearing on August 28, 2018, and the hearing was convened as scheduled on September 26, 2018. The Government

offered eight exhibits, referred to as Government Exhibits 1 through 8, which were admitted without objection. The Applicant offered no exhibits at the hearing. He testified on his own behalf. DOHA received the transcript of the hearing (Tr.) on October 4, 2018.

Findings of Fact

Applicant is 60 years old. He is married with one biological child, and three children through the marriage. He has a Bachelors' degree. He holds the position of Engineer for a defense contractor. He seeks to retain a security clearance in connection with his employment in the defense industry.

Paragraph 1 Guideline K – Handling Protected Information The Government alleges that the Applicant is ineligible for clearance because of his deliberate failure to comply with rules and regulations for handling protected information-which includes classified and other sensitive government information, and proprietary information, which raises doubt about his trustworthiness, judgment, reliability, or willingness and ability to safeguard protected information.

Paragraph 2 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.

Paragraph 3 Guideline E - Personal Conduct The Government alleges that the Applicant is ineligible for clearance because his conduct involves questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations that raise questions about his reliability, trustworthiness and ability to protect classified information or sensitive information.

Applicant has worked in the defense industry for the past thirty-five years, and has held a security clearance for almost that entire time. He began working for his current employer in 2002. For the last 15 years, he has worked daily with classified information. Between 2013 and 2016, Applicant committed at least six separate security violations, five of which are alleged in the SOR. On each occasion, he was counseled and disciplined by his company for his misconduct.

His first security violation occurred in November 2013. While working with his current employer, he failed to comply with his company security manual requirements by failing to set the alarm for Closed Area (HB-322A), a classified area where he worked. (Government Exhibit 3.) His second violation occurred in December 2014. Again, Applicant failed to comply with his company security manual requirements and failed to set the alarm for Closed Area (HB-322B), a classified area. After each security violation, Applicant was counseled, written up, and disciplined for his misconduct. (Government Exhibit 4.)

The third security violation occurred in February 2015. This time, Applicant failed to comply with his company's Approved Trusted Download requirements by authorizing a trusted download to be conducted in an unauthorized format, in violation of the requirement. Applicant explained that he was authorized to conduct approved trusted downloads. On this occasion, he reviewed a document that one of his co-workers wanted to convert from Secret to unsecured. Applicant neglected to remember that he is prohibited from performing a trusted download on a word document where there is no potential for metadata to be hidden. The security violation was reported and written up. Applicant was counseled and disciplined for his misconduct. (Government Exhibit 5.)

Applicant's fourth security violation occurred in November 2015. This time, Applicant authorized an unclassified PowerPoint presentation that was later discovered to include classified information. He emailed the document to several Boeing employees at two Boeing locations. This resulted in a data spill in violation of Federal and company security regulations. From the investigation, the program security team determined that the classified information was compromised. Government Exhibit 8 and Tr. p. 30.) The security violation was reported and written up. Applicant was counseled and disciplined for his misconduct.

In December 2015, Applicant committed another security violation that was not alleged in the SOR, but which has important ramifications here. This violation was similar to the one he committed in November 2015, where Applicant believed the document to be an unclassified PowerPoint that he sent to a few co-workers. In this case, it was later determined by the company program protection security team that the document contained classified information. (Government Exhibit 7.) Applicant stated that the reason he did not question his actions is because he wrote the document, and felt that he had sufficient expertise and knowledge of the subject. (Tr. pp. 31 - 21.) The security violation was written up. Applicant was counseled and disciplined by his company for this misconduct.

In January 2016, Applicant committed his sixth and most recent security violation. This time, once again, he failed to set the alarm for Closed Area (HB-322B), the classified area where he works. The security violation was written up. Applicant was counseled and disciplined by his company for this misconduct. (Government Exhibit 6.)

In February 2017, Applicant's security clearance was suspended. Applicant contends that since his last security violation he has made significant changes to his behavior. He admits that he had been over confident and foolish about his ability to accomplish his responsibilities without mistakes. To reduce the risk of mistakes in the future, he has given up the responsibility of opening and closing the classified laboratories, which means that he no longer has the responsibility to alarm the laboratories. He has also given up performing trusted downloads. He believes that he has learned his lesson from these security violations. Applicant states that he is embarrassed and humiliated about his clearance suspension as it is an important part of his job.

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 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 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 K – Handling Protected Information

The security concern for Handing Protected Information is set out in AG ¶ 33, as follows:

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.

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

(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;

(c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium;

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

(h) negligence to lax security practices that persist despite counseling by management; and

(i) failure to comply with rules and regulations that results in damage to the national security, regardless of whether it was deliberate or negligent.

The evidence is sufficient to raise the above disqualifying conditions.

None of the mitigating conditions under AG ¶ 35, are applicable. (a) The behavior was recent and happened frequently, and casts doubt on Applicant's current reliability, trustworthiness and good judgment. (b) Applicant has not responded favorably to counseling (c) the security violations were not due to improper or inadequate training or unclear instructions, and (d) the violations was not inadvertent and there is evidence of compromise.

Applicant's recent carelessness and negligent conduct resulted in the commission of six security violations within a short period of time. He failed to lock his classified work area on four separate occasions, and on two others, he made serious errors when performing approved trusted downloading. The most recent of these security violations occurred in January 2016. Until recently, his over confident attitude

toward these violations made it difficult, if not impossible, for him to see his faults or to realize the seriousness of his mistakes. On each occasion, he was counseled and disciplined by his company. On two occasions, it was determined by his company that he had compromised classified information. This misconduct is unacceptable. At this time, Applicant has not demonstrated sufficient reform and rehabilitation at this time to meet the eligibility requirements for access to classified information.

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. Five are potentially applicable in this case:

> (b) unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such a system;
>
> (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;
>
> (g) negligence or lax security practices in handling information technology that persists despite counseling by management; and
>
> (h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

The evidence is sufficient to raise the above disqualifying conditions.

None of the mitigating conditions under AG ¶ 41 are applicable: (a) the behavior was recent and casts doubt on the individual's reliability, trustworthiness, or good

judgment; (b) the security violations were not minor and were not done solely in the interest of organizational efficiency and effectiveness; (c) the conduct was not unintentional or inadvertent and was not followed by a prompt, good faith effort to correct the situation, and by notification to appropriate personnel; and (d) the misuse was not due to improper or inadequate training or unclear instructions.

Applicant's history of negligence resulting in six security violations is recent, repetitive, serious, and concerning. His over confidence has been a risk to the national security, as it was determined that on two occasions he compromised classified information. The six security violations outlined in detail above show that he has not established sufficient mitigation under this guideline.

Guideline E, Personal Conduct

The security concern for Personal Conduct is set out in AG ¶ 15, as follows:

Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise question about an individuals' reliability, trustworthiness, and ability to protect classified or sensitive information.

Conditions that may be disqualifying under AG¶ 16 include:

16(c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, 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; and
>
> (3) a pattern of dishonesty or rule violations.

The evidence above is sufficient to raise the above disqualifying conditions.

None of the mitigating conditions under AG ¶ 17 are applicable. (a) the individual did not make prompt, good faith efforts to correct the problem; the failure to cooperate was not caused by advice from legal counsel or another advising individual; (c) the offenses were not minor, but recent, the behavior was not infrequent, nor did it happened under such unique circumstances that it is unlikely to recur, and it does cast doubt on the individuals reliability, trustworthy, or good judgment; (d) the individual acknowledged the behavior, but counseling has not been helpful; (e) the individual has taken some steps to reduce or eliminate vulnerability to exploitation, manipulation, or

duress, but it is not sufficient to mitigate this security concern; (f) and (g) are not at all applicable. Given Applicant's extensive work history in the defense department, and his experience working with classified information, his history of six recent security violations that occurred between 2013 and 2016 is personal conduct that demonstrates questionable judgment, untrustworthiness, unreliability, and unwillingness to comply with company and DoD rules and regulations. This pattern of repeated security violations is inexcusable.

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 K, Guideline M, and Guideline E 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 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 section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraph 1.a.:	Against Applicant
Subparagraph 1.b.:	Against Applicant
Subparagraph 1.c.:	Against Applicant

Subparagraph 1.d.:	Against Applicant
Subparagraph 1.e.:	Against Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 1.a.:	Against Applicant
Paragraph 3, Guideline E:	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