DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 12-03402
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Philip J. Katauskas, Esquire, Department Counsel
For Applicant: *Pro se*

February 26, 2016

Decision

CEFOLA, Richard A., Administrative Judge:

Applicant submitted his Electronic Questionnaires for Investigations Processing (e-QIP) on October 7, 2011. On October 3, 2014, the Department of Defense (DOD) issued a Statement of Reasons (SOR) detailing the security concerns under Guidelines K, M and E for Applicant. The action was taken under Executive Order 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 within the Department of Defense after September 1, 2006.

Applicant answered the SOR in writing on October 28, 2014, and requested an Administrative Determination by an administrative judge. Department Counsel issued a File of Relevant Material (FORM) on September 29, 2015. Applicant responded to the FORM on October 23, 2015, with a one page unsworn, written statement by Applicant. Department Counsel had no objection to this written statement. The case was assigned to me on November 10, 2015. Based upon a review of the pleadings and exhibits, eligibility for access to classified information is denied.

Findings of Fact

In his Answer to the SOR, Applicant admitted all the factual allegations in the Subparagraphs of the SOR, with explanations; except for subparagraph 3.b., in that he denies falsifying any "material facts" on his October 2011 e-QIP. (Item 4.)

Applicant is a 57-year-old employee of a defense contractor. (Item 5 at pages 5 and 10.) He received a "Doctorate" degree in 1999, and is employed as a "Director of Technology." (Item 5 at pages 9~10.)

Guideline K - Handling Protected Information & Guideline E - Personal Conduct

1.a. and 3.a. Applicant admits, that in 2007, he knowingly and improperly transmitted classified information via email "to his unclassified work computer." (Item 7.) He did not report this incident until January 18, 2011, three days before his January 21, 2011 polygraph. (*Id*.) Applicant admits that this was a security violation, but denies he later "falsified material facts" vis-a-vis this violation.

Guideline M - Use of Information Technology Systems & Guideline E - Personal Conduct

2.a. and 3.a. Applicant admits that sometime prior to his January 21, 2011 polygraph, he accessed and viewed pornographic material on his work computer. (Item 6 at page 2.) He received a written reprimand as a result of this improper use of his information technology system, his work computer.

Guideline E - Personal Conduct

3.b. In answer to **Section 13A - Employment Activities - Received Discipline or Warming**, Applicant disclosed his 2011 written reprimand as a result of his viewing pornography on his work computer, as noted above. As to his 2007 security violation, he avers the following: "I received no written warning, official reprimand, suspension, or disciplinary action. I remember being a bit puzzled that there was no question on the SF-86 that flat out asked if I had any security violations on record." (Item 4.) I find no wilful falsification here, as the Government failed to establish he "received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace," which is what Section 13A requires to be disclosed.

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 useful 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, these guidelines are applied in conjunction with the factors listed in the adjudicative process. (AG Paragraph 2.) The administrative judge's

over-arching adjudicative goal is a fair, impartial and commonsense decision. According to AG Paragraph 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 Paragraph 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information 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. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Under Directive Paragraph E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive Paragraph E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion as to obtaining 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 Executive Order 10865 provides that 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 relating to the guideline for Handling Protected Information is set out in AG Paragraph 33:

> Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgement, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

The guideline notes several conditions that could raise security concerns. Under Subparagraph 34(c), ". . . *transmitting . . . classified reports, data, or other information*

on any unapproved equipment" is potentially disqualifying. Similarly under Subparagraph 34(g), *"any failure to comply with rules for the protection of classified or other sensitive information*" may raise security concerns. Applicant violated security by his improper transmission of classified information in 2007. This violation was compounded by his failure to disclose it until faced with a polygraph in 2011. I find no countervailing Mitigating Condition that is applicable here. Under Subparagraph 35 (a), when "*so much time has elapsed since the behavior . . . that is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment, . . .*" such facts may be mitigating. Although Applicant's initial violation occurred in 2007, he failed to disclose it until 2011. For more than three years he had every opportunity to do so, but chose not to. Handling Protected Information is found against Applicant.

Guideline M - Use of Information Technology Systems

Paragraph 39 of the adjudicative guidelines sets out the security concern relating to Use of Information Technology Systems:

> Noncompliance 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.

The adjudicative guidelines again set out certain conditions that could raise security concerns. Paragraph 40(e) provides that "unauthorized use of a government or other information system," may also raise security concerns. Here, he downloaded pornography to his work computer**.**

Again, I find no mitigating condition that is applicable here. Paragraph 41(a)provides that it may be mitigating where "so much time has elapsed since the behavior . . . that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment." The Applicant's improper conduct occurred sometime prior to him executing his 2011 e-QIP; but when coupled with his mishandling of protected information noted above, it is too soon to say it does not cast doubt on the individual's current reliability, trustworthiness, or good judgment**.**

Guideline E - Personal Conduct

The adjudicative guidelines set out the security concern relating to Personal Conduct in Paragraph 15:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations" could indicate that the person may not properly safeguard information.

The adjudicative guidelines set out certain conditions that could raise security concerns. Paragraph 16(d) arguably applies and provides that "credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, 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 (3) a pattern of dishonesty or rule violations" may be disqualifying. Here, the Appellant improperly transferred classified information, he failed to divulge his improper transfer for at least three years until faced with a polygraph, and he knowingly viewed pornography for which received a written reprimand. I find no countervailing mitigating conditions that are applicable here.

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 Applicant's conduct and all the circumstances. Under Paragraph 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.

The administrative judge should also consider the nine adjudicative process factors listed at AG Paragraph 2(a):

> (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.

I considered all of the evidence, including the potentially disqualifying and mitigating conditions surrounding this case. The record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For this reason, I conclude Applicant has not mitigated the security concerns arising from his Handling of Protected Information, his Use of Information Technology, and his Personal Conduct under the whole-person concept.

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

Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.a.	Against Applicant
Paragraph 3, Guideline E:	AGAINST APPLICANT
Subparagraph 3.a.	Against Applicant
Subparagraph 3.b.	For 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 eligibility for a security clearance. Eligibility for access to classified information is denied.

Richard A. Cefola
Administrative Judge