DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[Redacted]	)	ISCR Case No. 16-03180
	)	
Applicant for Security Clearance	)	

Appearances

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

12/18/2017

Decision

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guidelines M (Use of Information Technology) and E (Personal Conduct). Security concerns raised by Applicant's misuse of information technology and violation of an agency photography policy are mitigated. Security concerns raised by his lack of candor during the security clearance process are not mitigated. Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on December 16, 2015. On December 6, 2016, the Department of Defense (DOD) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines M and E. The DOD acted under Executive Order (Exec. Or.) 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) implemented by DOD on September 1, 2006.[1]

Applicant answered the SOR on January 9, 2016, and requested a decision on the record without a hearing. Department Counsel's submission of the Government's written is undated. It was sent to Applicant on August 14, 2017, along with a complete copy of the file of relevant material (FORM), and he was given an opportunity to file objections and submit material to refute, extenuate, or mitigate the Government's evidence. He received the FORM on August 21, 2017, and but did not submit any additional information. The case was assigned to me on December 18, 2017.

Findings of Fact[2]

In Applicant's answer to the SOR, he admitted all the allegations except SOR 2.c, alleging falsification of his SCA, which he denied. His admissions are incorporated in my findings of fact.

Applicant is a 35-year-old information technology systems administrator employed by a defense contractor since August 2015. He received a bachelor's degree in May 2009. He worked as a systems administrator associate for a defense contractor from January 2011 to March 2012. He was unemployed for about a month in April 2012. He worked as a systems administrator for federal contractor supporting another government agency (AGA) from May 2012 to May 2014. He was unemployed from June 2014 to January 2015, after his access to the AGA work site was revoked because of the conduct alleged in SOR ¶¶ 1.a, 1.b, and 2.a. He worked as a systems administrator for another defense contractor from February to April 2015, and was unemployed from May to July 2015, when he began his current employment. He received a security clearance in January 2011.

Around April 1, 2014, Applicant used his privileges as a system administrator to use his employer's computer to gain access to co-workers' computers and open their CD-ROM trays as an April Fools' Day prank. On the same day, he took pictures of himself, his computer monitor displaying the command he used for the prank, as well as other random items at his work site, and he posted them on social media. One of the "selfie" photographs included a sign identifying the AGA. Taking photographs of the work site was prohibited by the AGA. The prank is alleged in SOR ¶¶ 1.a, 1.b, and 2.b; and his violation of the photography policy is alleged in SOR ¶ 2.a.

[1] Security Executive Agent Directive 4 (SEAD 4), was issued on December 10, 2016, revising the 2006 adjudicative guidelines for all adjudicative decisions issued on or after June 8, 2017. The revision included changing the title of Guideline M from "Use of Information Technology Systems" to "Use of Information Technology." The changes resulting from issuance of SEAD 4 did not affect my decision in this case.

[2] Applicant's personal information is extracted from his security clearance application (FORM Item 4) unless otherwise indicated by a parenthetical citation to the record.

Applicant's violation of the photography policy was reported to the AGA security office by a person not identified in the record. Applicant was questioned by an AGA investigator, initially denied taking photographs at the work site, and later admitted it.

When Applicant submitted his SCA in December 2015, he answered "No" to the question whether, in the last seven years, he had illegally or without proper authorization accessed or attempted to access any information technology system. He did not disclose his April Fools' Day prank. His failure to disclose the prank is alleged in SOR ¶ 2.c. In his response to the SOR, he admitted that his "No" answer was incorrect, but he explained that he entered the wrong answer in the SCA because he was rushed and did not read the question carefully.

During an interview with a security investigator in June 2016, Applicant was questioned about his negative answer in the SCA, and he did not disclose the April Fools' Day prank until he was confronted with the evidence. His initial failure to disclose the incident during the security interview is alleged in SOR ¶ 2.d.

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.

Eligibility for a security clearance 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 all available and reliable information about the person, past and present, favorable and unfavorable.

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. *See 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* ISCR Case No. 15-01253 at 3 (App. Bd. Apr.20, 2016).

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* 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.

Analysis

Guideline M, Use of Information Technology

The concern under this Guideline is set out in AG ¶ 39:

> 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 following disqualifying conditions under this guideline are potentially applicable to Applicant's April Fools' Day prank:

AG ¶ 40(a): unauthorized entry into any information technology system;

AG ¶ 40(c): use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system; and

AG ¶ 40(e): unauthorized use of any information technology system;

All the disqualifying conditions are established. Applicant was authorized as a system administrator to gain access to his co-workers' computers, but not for the purpose of playing a prank.

The SOR ¶ 1.a alleges that Applicant's access to the AGA work site was revoked because of the conduct alleged in SOR ¶ 1.b. When the same conduct is alleged twice in the SOR under the same guideline, one of the duplicative allegations should be resolved in Applicant's favor. *See* ISCR Case No. 03-04704 (App. Bd. Sep. 21, 2005). Accordingly, I have resolved SOR ¶ 1.b in Applicant's favor.

The following mitigating conditions are potentially applicable:

AG ¶ 41(a): so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and

AG ¶ 41(b): the misuse was minor and done solely in the interest of organizational efficiency and effectiveness.

AG ¶ 41(a) is established. Applicant's prank was an isolated incident that happened more than three years ago. He lost his job because of the prank and is not likely to repeat his conduct.

AG ¶ 41(b) is not established. Although Applicant's prank was a minor violation, it was not done for organizational efficiency or effectiveness.

Guideline E, Personal Conduct

The concern under this guideline is set out in 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. . . .

Applicant's lack of candor during questioning by the AGA investigator, in his SCA, and during the follow-up interview with a security investigator establish the following disqualifying conditions under this guideline:

> AG ¶16(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; and
>
> AG ¶16(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.

Applicant's April Fools' Day prank is cross-alleged under this guideline in SOR ¶ 2.b. The evidence of his prank establishes the following disqualifying condition:

> AG ¶ 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.
>
> The following mitigating conditions are potentially applicable:
>
> AG ¶ 17(a): the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts; and
>
> AG ¶ 17(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.

AG ¶ 17(a) is not established for Applicant's false statements during questioning by the AGA investigator, in his SCA, and during the security interview in June 2016. Applicant did not correct his falsifications until he was confronted with the evidence.

AG ¶ 17(c) is established for Applicant's April Fools' Day prank. It was an isolated incident that occurred more than three years ago, and it was harmless from a security viewpoint. This mitigating condition is established for Applicant's violation of the AGA's photography policy. It was a violation of security procedures and not minor, but it was an

isolated incident that that occurred more than three years ago. This mitigating condition is not established for Applicant's falsifications, which undermined the security clearance process and occurred on three occasions.

Whole-Person Concept

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. In applying the whole-person concept, an 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 and applying the adjudicative factors in AG ¶ 2(d).[3]

I have incorporated my comments under Guidelines M and E in my whole-person analysis and applied the adjudicative factors in AG ¶ 2(d). Applicant presented no information regarding the quality of his performance in his current job. Because he requested a determination on the record without a hearing, I had no opportunity to evaluate his credibility and sincerity based on demeanor. *See* ISCR Case No. 01-12350 at 3-4 (App. Bd. Jul. 23, 2003). After weighing the disqualifying and mitigating conditions under Guideline M and E, and evaluating all the evidence in the context of the whole person, I conclude Applicant has mitigated the security concerns raised by his misuse of information technology, but he has not mitigated the security concerns raised by his lack of candor in response to questioning about his misconduct.

Formal Findings

I make the following formal findings on the allegations in the SOR:

Paragraph 1, Guideline F (Information Technology):	FOR APPLICANT
Subparagraphs 1.a and 1.b:	For Applicant
Paragraph 2, Guideline E (Personal Conduct):	AGAINST APPLICANT
Subparagraphs 2.a and 2.b:	For Applicant
Subparagraphs 2.c and 2.d:	Against Applicant

[3] The 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.

Conclusion

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

LeRoy F. Foreman
Administrative Judge