DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 14-02814
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Charles C. Hale, Esq., Department Counsel
For Applicant: *Pro se*

08/16/2017

Decision

MURPHY, Braden M., Administrative Judge:

Applicant mitigated the security concerns under Guideline E, personal conduct, and Guideline K, handling protected information, due to the isolated nature of the incident and the passage of time without evidence of recurrence. Applicant's eligibility for continued access to classified information is granted.

Statement of the Case

On July 13, 2016, the Department of Defense Consolidated Adjudications Facility (DoD CAF) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline E, personal conduct, and Guideline K, handling protected information. The action was taken 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 effective within the DOD on September 1, 2006.

On December 10, 2016, the Director of National Intelligence (DNI) issued Security Executive Agent Directive 4, National Security Adjudicative Guidelines (AG). The new AGs became effective on June 8, 2017, for all adjudicative decisions on or after that date.[1] Any changes resulting from the implementation of the new AGs did not affect my decision in this case.

Applicant answered the SOR on August 1, 2016. He requested a decision based on the written record in lieu of a hearing. On September 28, 2016, Department Counsel submitted the Government's File of Relevant Material (FORM), including documents identified as Items 1-7. Applicant received the FORM on October 4, 2016. He was afforded an opportunity to file objections and submit material in refutation, extenuation, or mitigation. Applicant did not respond to the FORM, and did not object to the Government's evidence. The SOR and the answer (Items 1 & 2) are the pleadings in the case. Items 3 through 7 are admitted without objection. The case was assigned to me on August 8, 2017.

Findings of Fact

Applicant admitted SOR ¶ 1.a, and the cross-allegation, ¶ 2.a, without comment. His admissions are incorporated into the findings of fact. After a thorough and careful review of the pleadings and exhibits submitted, I make the following additional findings of fact.

Applicant is 43 years old. He was born in Vietnam in 1974. He came to the United States as an infant, with his parents and siblings in 1975. He was raised and educated in the United States. He earned a bachelor's degree in 2000, and married the same year. He became a United States citizen in 2003. (Item 3)

Applicant has worked as a manufacturer for his employer, a large defense contractor, since 2002. He submitted a security clearance application (SCA) in January 2011. He stated he was granted a secret clearance in April 2011. (Items 3, 5)[2]

In May 2011, the Defense Industrial Security Clearance Office (DISCO) requested that Applicant's security clearance be suspended. The underlying rationale was given as follows:

> [In December 2010], subject broke company policy by taking a photograph with his personal telephone, in an area where photography is prohibited. The subject took a photograph of a sensitive item, in an area where he

[1] The new Adjudicative Guidelines are available on the DOHA website at http://ogc.osd.mil/doha/5220-6_R20170608.pdf.

[2] There is no documentation from the Government specifying the date Applicant's clearance was granted.

had no logical reason for being.[3] The subject's actions raise serious concerns regarding his reliability and trustworthiness concerning the protection of classified information. His continued access to classified information is not clearly consistent with the interests of national security.[4]

In June 2011, DISCO suspended Applicant's clearance. (Item 7) In September 2011, Applicant provided an affidavit to a special agent of the U.S. Office of Personnel Management (OPM) (Item 5) in which he described the incident as follows:

> In May or June 2011 [sic],[5] I had an incident regarding a camera phone. Camera phones were previously not allowed in the building at all. The policy changed and now camera phones are allowed. I understood I was not allowed to take pictures of any parts we build, but did not think it was a problem to take a picture of a machine because machines are everywhere. I took a picture of [name of item]. My son asked how parts are made and I said this machine makes the parts and can make anything. I took a picture of the machine to show my son.
>
> The operator was standing there and said, "Hey, you can't take a picture of that." I said OK and deleted the picture. The operator went to his supervisor, [name] and told him about me taking the picture. [The supervisor] sent me an e-mail asking if I had taken a picture. I spoke with [the supervisor] and showed him the phone where I had deleted the picture. I then took the initiative to call security . . . . I told [security] what I did because I was not trying to hide anything. The security person . . . said to delete the picture which I had already done and told me not to do it again.[6]

Applicant then went to the security office, where he received a written copy of the company policy about camera use.

> I was not previously given any training on this and did not know that I was not supposed to use the camera phone for any reason. Security told me it

[3] The SOR did not allege that Applicant had no reason to be in the area where he took the photograph, and the Government did not provide any argument or evidence (beyond this reference in Item 6) that this was the case.

[4] Item 6.

[5] Relying on this date, the Government argues that Applicant took the picture "immediately on being granted a clearance," in April 2011, thereby calling into serious question his suitability to hold one. FORM at 3. I find, however, that the incident occurred in December 2010, as alleged in the SOR, and as referenced in the memo prepared by DISCO, the government security office tasked with investigating the incident. (Items 1, 6) Applicant therefore took the picture before he was granted a clearance, and before he applied for one. However, my decision would be the same if the incident occurred in 2011.

[6] Item 5.

> was [prohibited] not just inside the facility, but also outside. If it is a rock, you can't take a picture. . . I now know the policy.[7]

Applicant indicated that he kept his supervisors informed. He was not reprimanded. He did not receive a security violation and was not "written up" for any misconduct. The next day, he met with his company's facility security officer. He filled out a form detailing what happened. With permission, he gave the camera policy to employees he worked with "so that it would be clear to them and no one would make the same mistake I did." (Item 5)

Applicant also said, "I regret taking the picture and it was a lesson hard learned." In August 2011, he learned his clearance was suspended. (Item 5)

In December 2013, Applicant was interviewed by another OPM agent. He largely repeated the general details of the incident with the camera phone, and his subsequent interactions with his supervisors and security officials. He also said he had no intentional security violations and did not knowingly violate policies. He had not had any previous or subsequent disciplinary incidents or performance concerns. He indicated that he had no intention of committing any future security violations.[8]

Guideline E SOR ¶ 1.a is set forth as follows:

> On December 14, 2010, you broke [name] company policy by taking a photograph of a sensitive item with your personal telephone, in an area where photography is prohibited. You received a letter of suspension as a result of this incident.

Applicant admitted the allegation (and the Guideline K cross-allegation, ¶ 2.a) without comment.[9] The record does not contain documentation from Applicant's employer regarding either the company policy in question, or whether Applicant knew about the policy before he took the picture.

Policies

It is well established that no one has a right to a security clearance. As noted by the Supreme Court in *Department of the Navy v. Egan*, "the clearly consistent standard indicates that security determinations should err, if they must, on the side of denials."[10]

---

[7] Item 5.

[8] The interview detailed in Item 4 occurred three years after the incident, so it is the only record evidence of later events.

[9] With his answer, Applicant included a cover letter, and stated, in part, "I hope I filled the form out correctly," but he made no substantive comments. Item 2.

[10] *Department of Navy v. Egan*, 484 U.S. 518, 531 (1988).

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are 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, these guidelines are applied 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(a), 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. Likewise, I have not drawn inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel and 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 safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information.

Analysis

In December 2010, Applicant used his personal cellphone to take an unauthorized picture of a machine at work, in an area where photography was prohibited. He took the photo in full view of the machine operator, who told him he should not have done it. Applicant promptly deleted the photo from his phone. He also reported the matter to supervisors, and cooperated fully with security. He does not appear to have been aware that there was a company policy against taking pictures of

anything at work, and there is no evidence to the contrary. As a matter of common sense, though, he probably should have known that it was poor judgment to take a picture of a machine at work with a personal cellphone.

Nevertheless, having been informed of the company policy and given a copy of it, Applicant took it to heart, and saw to it that his own employees were informed about it so they would not make the same mistake he did. He informed his supervisors, cooperated with security and responded well to their instructions, and expressed regret for his action. There is no indication that this is anything other than a one-time incident.

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern for personal conduct:

> 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. The following disqualifying conditions are potentially applicable:

> (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;
>
> (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; and

(2) any disruptive, violent, or other inappropriate behavior;

In December 2010, Applicant took a picture of a machine at work, with his personal camera phone, without authorization, in an area where photography was prohibited. This act calls into question his judgment, trustworthiness and reliability. AG ¶¶ 16(c), 16(d)(1), and 16(d)(2) are therefore satisfied.

AG ¶ 17 sets forth the applicable mitigating conditions under Guideline E:

> (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.

The above mitigating conditions fully apply. Applicant took the photo in full view of the machine's operator, who promptly told him he should not have done it and to delete the picture. Applicant did so. He reported the matter to supervisors and to security, and cooperated fully. He indicated he was not aware of the company's policy prohibiting the taking of any pictures at work until after the incident, when he was given a copy of it.

This incident occurred more than five-and-a-half years before the SOR was issued. There is no indication that it has been repeated. Applicant acknowledged what he did, expressed regret for his action, cooperated fully, and responded favorably to subsequent guidance and counseling from supervisors and security officials. This was an isolated incident that is unlikely to recur. AG ¶¶ 17(c) and (d) fully apply.

Guideline K, Handling Protected Information

AG ¶ 33 details the Guideline K 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.

Security clearance cases require administrative judges to assess whether an applicant has the requisite good judgment, reliability, and trustworthiness to be

entrusted with classified information. When evidence is presented that an applicant previously mishandled classified information or violated a rule or regulation for the protection of protected information such an applicant bears a heavy burden in demonstrating that they should once again be found eligible for a security clearance.[11]

AG ¶ 34 describes conditions that could raise a security concern and may be disqualifying. The following disqualifying conditions are potentially applicable:

> (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;
>
> (d) inappropriate efforts to obtain or view protected information outside of one's need to know; and
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information;

The machine Applicant photographed was proprietary, and was in an area where photography was prohibited. The machine therefore constituted protected information. The personal cell phone he used was "unauthorized equipment" and an "unauthorized location" on which to store the image, however briefly. Applicant's action, satisfies the above AGs.

I also considered the conditions that could potentially mitigate security concerns in AG ¶ 35:

> (a) so much time has elapsed since the behavior, or it happened so infrequently or under such unusual circumstances that it is unlikely to recur or 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; and
>
> (d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

[11] ISCR Case No. 11-12202 at 5 (App. Bd. June 23, 2014) (very heavy burden standard); ISCR Case No. 01-25941 at 5 (App. Bd. May 7, 2004) (security clearance determinations are "not an exact science, but rather predicative judgments.").

The above mitigating conditions fully apply for the same reasons as set forth under Guideline E.

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 Guidelines E and K in my whole-person analysis. Overall, the record evidence leaves me with no questions or doubts as to Applicant's continued 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:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2: Guideline K:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

In light of all of the circumstances, presented by the record in this case, it is clearly consistent with the interests of national security to grant Applicant's continued

access to classified information. Eligibility for continued access to classified information is granted.

_____
Braden M. Murphy
Administrative Judge