DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[Redacted]	)	ISCR Case No. 19-02686
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Alison O'Connell, Esq., Department Counsel
For Applicant: Leon J. Schachter, Esq.

03/24/2020

_____

Decision

_____

FOREMAN, LeRoy F., Administrative Judge:

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

Statement of the Case

Applicant submitted a security clearance application on March 26, 2018. On November 15, 2019, the Department of Defense Consolidated Adjudications Facility (DOD CAF) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines M and E. 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) promulgated in Security Executive Agent Directive 4, *National Security Adjudicative Guidelines* (December 10, 2016), for all adjudicative decisions on or after June 8, 2017.

Applicant answered the SOR on December 13, 2019, and requested a hearing before an administrative judge. Department Counsel was ready to proceed on January

22, 2020, and the case was assigned to me on January 23, 2020. On February 3, 2020, the Defense Office of Hearings and Appeals (DOHA) notified Applicant that the hearing was scheduled for February 19, 2020. Applicant retained an attorney, who requested that the hearing be postponed until at least March 2, 2020. (Hearing Exhibit (HX) I at 3-4.) On February 18, 2020, I granted the request for postponement. (HX II.) On February 28, 2020, DOHA notified Applicant and his attorney that the hearing was rescheduled for March 9, 2020. On the same day, I issued a case management order requiring the parties to submit their witness lists and exhibits to me not later than February 18, 2020. (HX III.) Both parties complied with the order. (HX IV.) I convened the hearing as rescheduled. Applicant waived the 15-day notice requirement in Directive ¶ E3.1.8. (Tr. 7.)

Government Exhibits (GX) 1 and 2 were admitted in evidence. GX 2 was admitted over Applicant's objection. Applicant testified, presented the testimony of three witnesses, and submitted Applicant's Exhibits (AX) A-1, A-2 and B, which were admitted without objection. I kept the record open until March 16, 2020, to enable him to submit additional documentary evidence. He timely submitted AX C, which was admitted without objection. DOHA received the transcript (Tr.) on March 17, 2020.

Evidentiary and Procedural Issues

Applicant objected to GX 2, a Joint Personnel Adjudication System (JPAS) incident report on the grounds that it is an adverse statement by a witness who is not available for cross-examination, that it is not an official government record, and that it is not a record prepared by Applicant's former employer in the ordinary course of business. Department Counsel argued that the document was admissible as a document prepared in the regular course of business under Directive ¶ E3.1.20. I overruled Applicant's objection on the ground that the JPAS incident report was prepared in the regular course of business by a defense contractor who had an obligation to report an incident that might affect the security eligibility of a cleared employee. (Tr. 18-23.) *See* NISPOM DoD 5220.22-M, Section 3, ¶ 1-302.a ("Contractors shall report adverse information coming to their attention concerning any of their cleared employees."). *See also* ISCR Case No. 15-02859 (App. Bd. Jun. 23, 2017.) (Police report containing hearsay admissible both as an official record under Directive ¶ E3.1.20 and as a public record under Federal Rule of Evidence 803(8)).

I also acknowledged that the weight of the JPAS incident report was lessened by multiple layers of hearsay and inability to question the source of the information. (Tr. 23.) In this case, the admissibility of the JPAS incident report is mooted by Applicant's admissions in his answer to the SOR and at the hearing, which were incorporated in my findings of fact set out below.

Before the hearing, Applicant requested that Department Counsel produce documentary evidence of the policy of Applicant's former employer forbidding the use of thumb drives to transfer information to or among company computers. (HX I at 4.) At the hearing, Department Counsel stated that she had no documentary evidence of the policy and had not requested it from Applicant's former employer. (Tr. 24-25.) The Directive ¶

E3.1.11 limits discovery by an applicant to "non-privileged documents and materials subject to control by the DOHA." If the policy was set out in a document, the document was not subject to control by the DOHA. Applicant and his witnesses at the hearing testified that they had not seen documentary evidence of the policy, but that they were informed during training that the use of thumb drives was prohibited. Applicant's admissions moot the issue, because he admitted that he knew that the use of thumb drives was prohibited. His admissions were incorporated in my findings of fact set out below.

In Applicant's request for postponement of the hearing, he asserted that he did not have a complete copy of Applicant's response to the SOR. (Hearing Exhibit (HX) I at 4.) At the hearing, Department Counsel asserted that she had provided a complete copy of Applicant's answer to Applicant's attorney, who conceded that she may have done so. I recessed the hearing to allow Applicant's attorney to examine my copy of Applicant's answer and Department Counsel's copy. After the recess, Applicant's attorney was satisfied that he had a complete copy of Applicant's answer.
(Tr. 8-11.)

Findings of Fact

In Applicant's answer to the SOR, he admitted all the allegations. At the hearing, his attorney moved to withdraw his answer to the SOR and substitute a modified answer to the SOR. (HX V.) I denied the motion to withdraw his answer to the SOR on the ground that there is no authority under the Directive permitting an applicant to withdraw an answer to the SOR. However, I granted Applicant's motion to the extent that I allowed him to submit explanations for his answer to the SOR. (Tr. 13-17.) His admissions in his original answer to the SOR, his modified answer in HX V, and at the hearing are incorporated in my findings of fact.

Applicant is a 56-year-old cyber-security analyst employed by a defense contractor since March 2018. He received a bachelor's degree in 1986. He was an employee of another government agency for about five years. (Tr. 37.) He was employed by another defense contractor from July 2003 to March 2018, when he was terminated for the conduct alleged in the SOR. He married in May 1998 and has five children, ages 20, 19, 18, 15, and 14. He has held a security clearance since about 1999. (Tr. 70.)

In September 2017, Applicant sent an email to a co-worker, asking her to allow him to use her security token to gain access to an unclassified server in order to perform system software patching and troubleshooting. The security token is a small piece of hardware with a USB plug on the end. (Tr. 86.) His security token had been recently reissued and could not be read by the server. The compliance date for updating the system was approaching, and the system would be taken offline if he could not complete the updates. (Tr. 58.) His co-worker declined, telling him that she would be uncomfortable allowing him to use her security token. His former employer's security team intercepted their email exchange. Applicant testified that he was given an alternate method of bypassing the token requirement, but it did not work. (Tr. 56-57.) He testified that he did

not ask his co-worker to install the security updates because she did not have the skill set required to install them. (Tr. 68.) He knew, based on training and the provisions of the non-disclosure agreement that he signed, that employees were not allowed to share credentials. (Tr. 71.)

Based on an internal investigation by the corporate counsel and facility security officer in January and February 2018, Applicant was terminated on March 2, 2018. (GX 2.) When Applicant submitted his most recent SCA in March 2018, he disclosed his termination and the attempt to use another employee's security token. (GX 1 at 15.)

Applicant testified that he had submitted multiple requests for almost a month to install a device driver that could read his new security token. (Tr. 41.) In the meantime, he was unable to install the patches and security updates necessary to protect the system from being hacked. (Tr. 44-45.) He testified that in hindsight he should have escalated his problem with his security token to his supervisors. (Tr. 47.) He testified that during the investigation the corporate counsel asked him if he would try to use someone else's security token again, and he said that he would "if it would get the job done." When reminded by the corporate counsel that he had signed a non-disclosure agreement prohibiting sharing of credentials, he responded, "Okay, I won't do it." (Tr. 64.)

Applicant testified that, in February 2018, the corporate counsel told him that they had observed his use of a personal thumb drive in September 2017 to transfer work-related data between his employer's unclassified information systems. (Tr. 60.) At the hearing, he admitted that he started using a thumb drive in April 2017, when his employer's system was migrated into a government system. He was having problems with downloading software updates and security patches. He knew how to clean a thumb drive to prevent transmitting malware. He did not connect the thumb drive to a government network. He used the thumb drive to transfer data from his contractor's laptop to his government laptop on four occasions, in April, July, September, and November 2017. (Tr. 47-49.) He testified that the SOR was inaccurate when it alleged that he used the thumb drive beginning in July 2003. The basis for alleging that Applicant used the thumb drive from July 2003 to March 2018 is not in the record. The inclusive dates of Applicant's unauthorized use of a thumb drive are not reflected in the JPAS incident report. He testified that when he answered the SOR, he stated that he admitted that he used the thumb drive between July 2003 and March 2018 because those were the dates of his employment by his former employer. He testified that he did not know that he could admit part of the allegation and deny part of it. (Tr. 50.)

Applicant testified that he has never seen a document forbidding the use of thumb drives. However, he admitted that during training he was clearly told that he should not use thumb drives. (Tr. 52, 62.) However, he believed that the permissible devices such as compact discs were the same as using a thumb drive and just as safe because he knew how to "nuke" the thumb drive and remove any potential contamination. (Tr. 52-54.)

The JPAS incident report (GX 2) recited that Applicant was cautioned against using the thumb drive and instructed to not use it again, and that "he replied that he could not

guarantee he would not do it again if he needed to accomplish his mission." Applicant denied telling the investigators that he could not guarantee that he would not use a thumb drive again. (Tr. 63-64.) He testified that he told the contractor's counsel that he would not use a thumb drive again but that he was uncomfortable leaving the system insecure. (Tr. 64.)

Applicant's use of a thumb drive and his attempt to use a co-worker's security token occurred only on unclassified systems. He testified that a classified system is totally different with very stringent rules. (Tr. 68.) He would never bypass security rules on a classified system for efficiency. He believes that the rules for classified systems are about security, not efficiency. (Tr. 65-66.)

The co-worker who declined Applicant's request to use her security token testified on his behalf. She has worked for Applicant's former employer as a software engineer since May 2007. She regards Applicant as very responsible, reliable, honest, and trustworthy. (Tr. 76-80.) She testified that Applicant's token had expired, and that she declined Applicant's request to use her token, telling him that she did not feel comfortable allowing him to use it and did not want to get their employer in trouble. She did not report his request. Her opinion of Applicant did not change as a result of his request. (Tr. 82, 86.)

Another former co-worker who had worked with Applicant on a project for about eight years testified that she believes he is a trustworthy, reliable, and honest person. She testified that their employer allowed the use of thumb drives about ten years ago, but the policy changed with the technology and everyone was notified by bulletins and emails of the change. She testified that she believes Applicant knows that he made a mistake and that he wants to do the right thing. (Tr. 90-96.)

A current co-worker has known Applicant for about four years and works with him on the same project. He considers Applicant to have good judgment and believes he is very reliable, trustworthy, and honest. He is aware of the reasons Applicant was terminated by his previous employer, but believes Applicant had no malicious intent, but "at the end of the day, he was just trying to get the job done." (Tr. 98-103.)

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 SOR alleges that in about September 2017, Applicant attempted to gain access to an information technology system by using another employee's security token

in violation of "company business ethics and operations standards" (SOR ¶ 1.a). It also alleges that between about July 2003 and March 2018, Applicant regularly used an unauthorized personal USB storage device to move work-related data to and from unclassified information systems in violation of "company business ethics and operations standards" (SOR ¶ 1.b).

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 relevant:

> AG ¶ 40(a): unauthorized entry into any information technology system;
>
> AG ¶ 40(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; and
>
> AG ¶ 40(g): negligence or lax security practices in handling information technology that persists despite counseling by management.

AG ¶ 40(a) is applicable but not fully established. Applicant attempted to gain entry into his employer's information technology system, but he was unsuccessful because his co-worker would not allow him to use her security token.

AG ¶ 40(f) is established. Applicant introduced an unauthorized personal thumb drive into his employer's information technology system.

AG ¶ 40(g) is not established. There is no evidence that Applicant was counseled about sharing security tokens or using a thumb drive. He testified that the corporate counsel told him that he had been observed using a thumb drive in September 2017, but there is no evidence that he was admonished or counseled until he was interviewed by the corporate counsel in February 2018.

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;
>
> AG ¶ 41(b): the misuse was minor and done solely in the interest of organizational efficiency and effectiveness; and
>
> AG ¶ 41(d): the misuse was due to improper or inadequate training or unclear instructions.

AG ¶ 41(a) is established. Applicant's infractions occurred more than two years ago and have not recurred in his current job. He has acknowledged his bad judgment and has suffered severe consequences for his infractions.

AG ¶ 41(b) is established. Both incidents involved minor infractions in the use of an unclassified system. Applicant's request to use a co-worker's security token was rebuffed and he did not pursue it. The use of a thumb drive previously had been permitted, but the company policy had changed. Applicant's sole motivation in both incidents was organizational efficiency and effectiveness. He made it clear during his testimony that he would have acted differently in a classified system.

AG ¶ 41(d) is not established. Applicant admitted in his answer to the SOR, his amended answer to the SOR, and his testimony at the hearing that he knew from his training that sharing of credentials and use of thumb drives were prohibited.

Guideline E, Personal Conduct

The SOR cross-alleges the conduct alleged in SOR ¶¶ 1.a and 1.b under this guideline (SOR ¶ 2.a). The security 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. . . ."

The following disqualifying conditions under this guideline are potentially applicable:

> 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; and

AG ¶ 16(f): violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

AG ¶ 16(c) is established by Applicant's repeated violations of the rules for use of his employer's information technology system. AG ¶ 16(f) is established by his repeated violation of the conditions he agreed to in his non-disclosure agreement.

The following mitigating conditions are potentially applicable:

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; and

AG ¶ 17(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.

AG ¶ 17(c) is established for the reasons set out in the above discussion of Guideline M. AG ¶ 17(d) is partially established. Applicant has acknowledged his behavior. There is no evidence of counseling or "other positive steps" taken by Applicant, but his behavior is unlikely to recur, for the reasons set out in the above discussion of Guideline M.

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): (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 have incorporated my comments under Guidelines M and E in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines, but some warrant additional comment. Applicant was candid, sincere, and credible at the hearing. He was not particularly remorseful. Instead, he conveyed the impression that he

thought his conduct was justified, but he also made it clear that he will not jeopardize his career by further violations. He has worked as a federal employee and a defense contractor for over 20 years and held a security clearance for more than 16 years. He is highly respected for his reliability. His infractions were motivated by a misguided decision to ignore less efficient rules in order to support his employer more efficiently. He has paid dearly for his disregard for security rules and appears to have learned his lesson. After weighing the disqualifying and mitigating conditions under Guidelines 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 violation of the rules for protecting information technology.

Formal Findings

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

Paragraph 1, Guideline M:	FOR APPLICANT
Subparagraphs 1.a and 1.b:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

I conclude that it is clearly consistent with the national security interests of the United States to continue Applicant's eligibility for access to classified information. Clearance is granted.

LeRoy F. Foreman
Administrative Judge