*The original of this document contains information which is subject to withholding from disclosure under 5 U.S. C. § 552. Such material has been deleted from this copy and replaced with XXXXXX's.

United States Department of Energy
Office of Hearings and Appeals

In the Matter of: Personnel Security Hearing	)		
	)		
Filing Date: January 22, 2021	)	Case No.:	PSH-21-0011
	)		
	)		

Issued: May 6, 2021

Administrative Judge Decision

Kimberly Jenkins-Chapman, Administrative Judge:

This Decision concerns the eligibility of XXXXXX (hereinafter referred to as "the Individual") for access authorization under the Department of Energy's (DOE) regulations set forth at 10 C.F.R. Part 710, entitled, "Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material."[1] For the reasons set forth below, I conclude that the Individual's security clearance should not be restored.

I. BACKGROUND

The Individual is employed by a DOE Contractor in a position that requires him to hold a security clearance. His security clearance was suspended after DOE discovered derogatory information about the Individual—that he had accessed, on a classified computer system and without authorization, a file cataloguing disciplinary counseling for employees in his department—bringing into question his personal conduct and use of workplace information technology systems. The Local Security Office (LSO) began the present administrative review proceeding by issuing a Notification Letter to the Individual informing him that he was entitled to a hearing before an Administrative Judge in order to resolve the substantial doubt regarding his eligibility to continue holding a security clearance. *See* 10 C.F.R. § 710.21.

The Individual requested a hearing and the LSO forwarded the Individual's request to the Office of Hearings and Appeals (OHA). The Director of OHA appointed me as the Administrative Judge in this matter on January 22, 2021. At the hearing I convened pursuant to 10 C.F.R. § 710.25(d), (e) and (g), the Individual presented the testimony of three witnesses. *See* Transcript of Hearing, Case No. PSH-21-0011 (hereinafter cited as "Tr."). The LSO submitted nine exhibits, marked as

[1] Under the regulations, "Access authorization" means an administrative determination that an individual is eligible for access to classified matter or is eligible for access to, or control over, special nuclear material." 10 C.F.R. § 710.5(a). Such authorization will also be referred to in this Decision as a security clearance.

Exhibits 1 through 12 (hereinafter cited as "Ex."). The Individual submitted eight exhibits, marked as Exhibits A through H.

II. THE NOTIFICATION LETTER AND THE ASSOCIATED SECURITY CONCERNS

As indicated above, the Notification Letter informed the Individual that information in the possession of the DOE created a substantial doubt concerning his eligibility for a security clearance. That information pertains to Guidelines E and M of the *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position*, effective June 8, 2017 (Adjudicative Guidelines). 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.

Guideline E (Personal Conduct) relates to conduct involving questionable judgment, lack of candor, or unwillingness to comply with rules and regulations, which raises questions about an individual's reliability, trustworthiness and ability to protect classified information. Any failure to provide truthful and candid answers during the security clearance process is of particular concern. Adjudicative Guidelines ¶ 15.

Guideline M (Use of Information Technology) relates to failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems, which raises 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. Adjudicative Guidelines ¶ 39.

In the Notification Letter, the LSO alleges:

(1) In 2018, the Individual received a three-day disciplinary suspension for engaging in the unauthorized use of a classified computer system and violating the facility's net user agreement when he accessed proprietary data and private information about employees;

(2) The Individual failed to fully cooperate with the investigation into the 2018 information technology incident when he gave evasive and non-credible answers to investigators;

(3) The Individual refused to provide security clearance investigators with information regarding his 2018 suspension and reaffirmed his refusal after investigators advised him that adjudicating officials may not be able to make an informed decision about his security clearance;

(4) In 2017, the Individual was disciplined for failing to attend the required number of exercise sessions during a six-month period.

Ex. 2. Accordingly, the LSO's security concerns under Guidelines E and M are justified.

III. REGULATORY STANDARDS

A DOE administrative review proceeding under Part 710 requires me, as the Administrative Judge, to issue a Decision that reflects my comprehensive, common-sense judgment, made after consideration of all of the relevant evidence, favorable and unfavorable, as to whether the granting or continuation of a person's access authorization will not endanger the common defense and security and is clearly consistent with the national interest. 10 C.F.R. § 710.7(a). The entire process is a conscientious scrutiny of a number of variables known as the "whole person concept." Adjudicative Guidelines ¶ 2(a). The protection of the national security is the paramount consideration. The regulatory standard implies that there is a presumption against granting or restoring a security clearance. *See Department of Navy v. Egan*, 484 U.S. 518, 531 (1988) ("clearly consistent with the national interest" standard for granting security clearances indicates "that security determinations should err, if they must, on the side of denials"); *Dorfmont v. Brown*, 913 F.2d 1399, 1403 (9th Cir. 1990), cert. denied, 499 U.S. 905 (1991) (strong presumption against the issuance of a security clearance).

The Individual must come forward at the hearing with evidence to convince the DOE that granting or restoring access authorization "will not endanger the common defense and security and will be clearly consistent with the national interest." 10 C.F.R. § 710.27(d). The Individual is afforded a full opportunity to present evidence supporting his eligibility for an access authorization. The Part 710 regulations are drafted so as to permit the introduction of a very broad range of evidence at personnel security hearings. Even appropriate hearsay evidence may be admitted. 10 C.F.R. § 710.26(h). Hence, an individual is afforded the utmost latitude in the presentation of evidence to mitigate the security concerns at issue.

The discussion below reflects my application of these factors to the testimony and exhibits presented by both sides in this case.

IV. FINDINGS OF FACT

At the hearing, the Individual presented the testimony of a former supervisor, a colleague, and his former shift supervisor.

The former supervisor testified that he supervised the Individual for several years and that the Individual was his best employee. Tr. at 16, 18. He testified that the Individual was very reliable for a variety of tasks and that the Individual stood out among his employees for trustworthiness. *Id.* at 18–22. He further testified that warnings for not meeting exercise session requirements were not uncommon and that, though he would have been the one to issue the warning to the Individual in 2017, he did not remember the details of it because it was not a significant issue. *Id.* at 24–26. The former supervisor also testified that if an employee in the Individual's position found sensitive material that was not secure, they were to secure it, rather than access and view the material. *Id.* at 30–33. He testified that the Individual had a good eye for detail and knew when things "just don't look right" in connection with his employment. *Id.* at 33–34.

The Individual's colleague had known the Individual since 2014. Tr. at 41. He trusted the Individual and found him reliable. *Id.* at 43. He testified that if a sensitive document was found accessible, they were to secure the document and report it to their supervisor. *Id.* at 48–49. He further testified that they were not to review sensitive materials they found. *Id.*

The Individual's former shift supervisor testified that the Individual was a good worker who always wanted to get things right. Tr. at 54. He testified that the Individual's Chief had instructed the Individual to direct the security investigator to the Chief if she had any questions about the information security incident. *Id.* at 56–57. He testified that about half of the employee's work unit had accessed the file the Individual accessed. *Id.* at 64. He testified that he only advised people to tell the truth during the internal investigation into the incident. *Id.* at 82. He further testified that the Individual had undergone training on "need to know" access to sensitive information after the incident, which supplemented the Individual's annual training on the topic. *Id.* at 59–60, 105.

The Individual testified that his supervisor had directed him to inform the security clearance investigator that he had been suspended and that she should go to the Chief for further details. Tr. at 121. He complied with those instructions. *Id.* at 123–24. He testified that the investigator told him it was his chance to explain his side of the story, but he directed her to the Chief and declined to answer further questions. *Id.* at 123–24, 149.The Individual testified that he now knows that a security clearance investigator's question supersedes any directive from his manager and that he regrets not explaining his directive. *Id.* at 125. He testified that, at the time, he did not attempt to clarify the supervisor's directive after the investigator asked about the incident. *Id.* at 160–61.

The Individual testified that he admitted to internal investigators that he opened nearly 20 files in the classified system and that he did not intentionally withhold any information. Tr. at 127–29. The Individual admitted at the hearing that he violated government policies when accessing the files. *Id.* at 133–34. He testified that, at the time, he believed that he was allowed to access any file which could be accessed from his office's homepage. *Id.* at 134.

The Individual testified that he knew during the private investigation that he could be terminated for not cooperating fully. Tr. at 140. He testified that the security clearance investigator twice advised him that his refusal to answer questions about the information technology incident may prevent officials from making an informed decision on his eligibility for a clearance. *Id.* at 149. He testified that the main file he accessed on four occasions contained derogatory information on more than 10 of his colleagues. *Id.* at 150. He testified that, at the time, he did not think there was anything wrong with reading about adverse counseling and discipline for many of his colleagues and that markings such as "classified" or "private" would not have deterred him from reading a file if he could open it. He testified that he was curious to see if information about him was included in the file. *Id.* at 151. The Individual testified that his supervisor did not tell him not to cooperate with the security clearance investigator. *Id.* at 152.

V. ANALYSIS

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 places a high degree of trust and confidence in individuals to whom it grants access authorization. Decisions include, by necessity, consideration of the possible risk that 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.

The issue before me is whether the Individual, at the time of the hearing, presents an unacceptable risk to national security and the common defense. I must consider all the evidence, both favorable and unfavorable, in a commonsense manner. "Any doubt concerning personnel being considered for access for national security eligibility will be resolved in favor of the national security." Adjudicative Guidelines ¶ 2(b). In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. Because of the strong presumption against granting or restoring security clearances, I must deny access authorization if I am not convinced that the LSO's security concerns have been mitigated such that restoring the Individual's clearance is not an unacceptable risk to national security.

A. Guideline M

Guideline M provides that the following conditions may mitigate Use of Information Technology security concerns: (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; (b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness; (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel; and (d) the misuse was due to improper or inadequate training or unclear instructions. Adjudicative Guidelines ¶ 41.

The Individual's misuse of the information system is relatively recent, and he still has access to the system. Further, I cannot find that the Individual's unauthorized viewing of the materials occurred under unusual circumstances. While the misuse did not involve national security information, it did involve privacy information about other employees that he should have known was not meant for his use, and which also may have been protected by the Privacy Act. This misuse, therefore, is not minor and the Individual stated that his interest was curiosity, not organizational efficiency or effectiveness. Indeed, the very fact that the Individual thought viewing disciplinary information about his colleagues was appropriate simply because it was accessible calls the Individual's judgment into question. The misuse was intentional and repeated, and the Individual had received training on "need to know" standards prior to the incident. Failure to pay attention to annual required training cannot be considered inadequate training. For the foregoing reasons, I cannot find that the Individual has resolved the Guideline M security concerns.

B. Guideline E

Guideline E provides that the following conditions (in relevant part) may mitigate Personal Conduct security concerns: (1) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts; (2) 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 (3) 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. Adjudicative Guidelines at ¶ 17(a), (c), (d).

The Individual did not make a prompt or good faith effort to correct his concealment, even after being told that his refusal to discuss his disciplinary incident may affect his ability to hold a security clearance. The Individual stated that he now knows that the federal investigation superseded his Chief's directive not to discuss his security infraction, however, he has not obtained counseling or training on decision-making that may improve his ability to handle such situations proactively in the future.

The offense at issue, refusing to discuss the details of an intentional breach of an information system containing classified information, is deeply serious and goes to the very heart of the security clearance suitability process. The system breach was serious enough to have raised a Guideline M concern. It is more directly relevant to the interests of national security than other incidents which the Individual did discuss. Concealing such an issue directly frustrated the government's ability to evaluate the Individual's risk and cannot be considered minor.

Once the Individual experienced the adverse effects of his concealment, he became compliant and shared details of the systems breach. In determining whether the Individual is likely to conceal or omit information in the future, we take particular notice that the Individual did not respond to a warning that his actions may generate adverse consequences. He only corrected his concealment after actually receiving the warned-of consequences. This indicates that the Individual has difficulty following rules and, even more troubling, properly assessing risk. His deficient risk assessment skills are also demonstrated by the fact that he opened over 20 documents on a classified system without knowing what information might be contained. When combined with the Individual's access to classified systems and his struggle to remember security training, the Individual's difficulty following rules and assessing risk pose an unacceptable risk to the national security. Accordingly, I cannot find that the Individual has resolved all of the Guideline E security concerns.[2]

VI. CONCLUSION

Upon consideration of the entire record in this case, I find that there was evidence that raised concerns regarding the Individual's eligibility for a security clearance under Guidelines E and M of the Adjudicative Guidelines. I further find that the Individual has not succeeded in fully resolving those concerns. Therefore, I cannot conclude that restoring DOE access authorization to the Individual "will not endanger the common defense and security and is clearly consistent with the national interest." 10 C.F.R. § 710.7(a). Accordingly, I find that the DOE should not restore access authorization to the Individual at this time.

The parties may seek review of this Decision by an Appeal Panel, under the regulation set forth at 10 C.F.R. § 710.28.

Kimberly Jenkins-Chapman
Administrative Judge

[2] I find that the Individual has resolved the Guideline E concern related to his exercise sessions, however, this is not sufficient to resolve the entirety of the Guideline E concerns.