*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 14, 2016	)
		) Case No.: PSH-16-0002
		)

Issued: May 19, 2016

Administrative Judge Decision

Wade M. Boswell, Administrative Judge:

This Decision concerns the eligibility of XXXXX (hereinafter referred to as "the individual") to hold an access authorization[1] under the Department of Energy's (DOE) regulations set forth at 10 C.F.R. Part 710, Subpart A, entitled, "General Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material." As fully discussed below, after carefully considering the record before me in light of the relevant regulations and Adjudicative Guidelines, I have determined that the individual's access authorization should be restored.

I. Background

The individual is employed by a DOE contractor in a position that requires her to hold DOE access authorization. In April 2015, she was notified that she had been randomly selected for a security-related polygraph examination. Subsequently, she attended a counterintelligence briefing for those who were scheduled to take their first polygraph examination, and attendees were encouraged to self-disclose any matters that might be related to the four security questions that would be asked during the polygraph. Later that day, the individual met with her employer's security office and disclosed two occasions on which she failed to properly secure a vault-type room (VTR) and a period of time during

[1] Access authorization is defined as "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 be referred to variously in this Decision as access authorization or security clearance.

which she had taken a prohibited personal electronic device into the VTR; she had not previously reported any of these events. She subsequently passed the polygraph examination.

Her employer reported these violations of security regulations to the Local Security Office (LSO). *See* Exhibit 3; Exhibit 4. Subsequently, the LSO conducted a personnel security interview (PSI) with the individual in September 2015. *See* Exhibit 7. Since the PSI did not resolve the security concerns with respect to the individual's failure to comply with security procedures and her failure to timely report these failures, the LSO informed the individual in a letter dated November 23, 2015 (Notification Letter), that it possessed reliable information that created substantial doubt regarding her eligibility to hold a security clearance. In an attachment to the Notification Letter, the LSO explained that the derogatory information fell within the purview of two potentially disqualifying criteria set forth in the security regulations at 10 C.F.R. § 710.8, subsections (g) and (l) (hereinafter referred to as Criterion G and Criterion L, respectively).[2] *See* Exhibit 1.

Upon her receipt of the Notification Letter, the individual exercised her right under the Part 710 regulations by requesting an administrative review hearing. *See* Exhibit 2. The Director of the Office of Hearings and Appeals (OHA) appointed me the Administrative Judge in the case and, subsequently, I conducted an administrative hearing in the matter. At the hearing, the LSO introduced eight numbered exhibits into the record and presented no witnesses. The individual, represented by counsel, introduced seven lettered exhibits (Exhibits A-G) into the record and presented the testimony of four witnesses, including that of herself. The exhibits will be cited in this Decision as "Ex." followed by the appropriate numeric or alphabetic designation. The hearing transcript in the case will be cited as "Tr." followed by the relevant page number.[3]

II. Regulatory Standard

A. Individual's Burden

A DOE administrative review proceeding under Part 710 is not a criminal matter, where the government has the burden of proving the defendant guilty beyond a reasonable doubt. Rather, the standard in this proceeding places the burden on the individual because it is designed to protect national security interests. This is not an easy burden for the individual to sustain. 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).

[2] See Section III below.

[3] OHA decisions are available on the OHA website at energy.gov/oha/office-hearings-and-appeals. A decision may be accessed by entering the case number in the search engine at energy.gov/oha/security-cases.

The individual must come forward with evidence to convince the DOE that granting or restoring his or her 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 or her 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). Thus, an individual is afforded the utmost latitude in the presentation of evidence to mitigate the security concerns at issue.

B. Basis for the Administrative Judge's Decision

In personnel security cases arising under Part 710, it is my role as the Administrative Judge to issue a Decision that reflects my comprehensive, common-sense judgment, made after consideration of all 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). I am instructed by the regulations to resolve any doubt as to a person's access authorization eligibility in favor of the national security. *Id.*

III. The Notification Letter and the Security Concerns at Issue

As previously noted, the LSO cited two criteria as the bases for suspending the individual's security clearance: Criterion G and Criterion L. Criterion G concerns information that a person has "failed to protect classified matter, or safeguard special nuclear material; or violated or disregarded security or safeguards regulations to a degree which would be inconsistent with the national security; or disclosed classified information to a person unauthorized to receive such information; or violated or disregarded regulations, procedures, or guidelines pertaining to sensitive information technology systems." 10 C.F.R. § 710.8(g). Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern. *See* Guideline K of the *Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, issued on December 29, 2005, by the Assistant to the President for National Security Affairs, The White House (Adjudicative Guidelines). With respect to Criterion G, the LSO cites the individual's acknowledgements during the PSI that: (1) she failed to properly secure a VTR on two occasions; (2) she brought a personal cell phone into a VTR on two occasions; and (3) she brought a personal electronic device into a VTR on a daily basis for approximately one-and-one-half to two years, for personal convenience and as a result of workplace frustrations. Ex. 1 at 3.

Criterion L concerns information that an individual has engaged in conduct "which tends to show that the individual is not honest, reliable, or trustworthy…." 10 C.F.R. § 710.8(l). 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 information. *See* Adjudicative Guidelines at Guidelines E and F. With respect to Criterion L, the LSO alleges, *inter alai*, that: (1) the individual chose not report her failures, on two occasions, to properly secure a VTR at the time of those occurrences, despite being aware of the reporting requirements, in order to avoid the "hassle" of an investigation; (2) she chose not to report having, on two occasions, brought a prohibited personal cell phone into a VTR, despite being aware of the reporting requirement, because she believed there had been no compromise of classified information; and (3) she deliberately brought a personal electronic device into a prohibited area on a daily basis for approximately one-and-one-half to two years, despite being aware that such device was prohibited, for personal convenience and as a result of workplace frustrations. Ex. 1 at 4.

In light of the information available to the LSO, the LSO properly invoked Criterion G and Criterion L.

IV. Findings of Fact

The individual acknowledges the factual accuracy of the matters alleged in the Notification Letter, although she believes that the LSO misstated aspects of the motivation for some of her actions. Tr. at 113-116, 119-120. In those instances, I have carefully considered the totality of the individual's testimony, the entirety of the written record, and the arguments presented by both the individual and the LSO in reaching the findings set forth herein.

Since the individual began working for a DOE contractor, her work has required access authorization. Her desk and office are located within a VTR, which also houses a laboratory. *Id.* at 72. Due to the nature of the worked performed in the VTR, the VTR is a security restricted area.

In early 2011, the individual began carrying a personal electronic device; this pocket-sized device had wireless networking capacity (which could be switched on or off), but did not have telephonic capacity. The individual used the device to listen to music and play games when in non-restricted areas of her workplace. While the device was permitted in such areas, it was prohibited within the VTR. For approximately one-and-one-half years (from early 2011 until mid-2012), the individual carried the device into the VTR on a daily basis, although she did not use it while in the VTR. *Id.* at 72-74. She was aware that this violated security regulations; however, she continued to do so and did not self-report her security violations at the time. At the time, she felt frustrated because she believed she was being "purposefully" underutilized by her then-supervisor; however, she also felt at the time that the device, in her pocket with its wireless capacity turned off, did not present a security harm or risk. *Id.* at 72-73.

In 2012, the individual replaced her personal electronic device with a cellular telephone that also performed all the functions of her electronic device. She viewed taking a cell phone into the VTR as unacceptable. *Id.* at 74-75. However, on two occasions in 2014, she unintentionally carried her cell phone into the VTR and, upon realizing that she had done

so, immediately took the cell phone out of the VTR. Since the cell phone had been present in the VTR for just a few seconds, while in "airplane mode" with no classified materials around, the individual decided not to report either of the violations to her employer's security office. *Id.* at 75-76.

The VTR is required to be locked with alarms set when it is unoccupied. *Id.* at 35. The individual performed this function multiple times each day. When this is not properly done, access to the VTR is still limited by a "swipe lock" (that is, access is limited to those approved persons who "swipe" their badge and enter a code for access); however, the alarms are not set. *Id.* at 17, 78-80. On one occasion in January 2015, the individual returned to the VTR and realized that she had not fully secured it. She had been away for less than an hour and no classified materials were visible in the space, so she decided not to report it to her employer's security office. *Id.* at 76-77. Approximately one month later, her supervisor found that the individual had not fully secured the VTR and that incident was also not reported. *Id.* at 78.

In April 2015, the individual received notice that she had been randomly selected for a security-related polygraph examination. *Id.* at 84. She attended a briefing by counterintelligence for those about to take a polygraph for the first time. Attendees were informed of the four questions that would be asked and advised that they should consider self-disclosing any issues related to those questions prior to the polygraph. *Id.* at 84-85. That afternoon, the individual met with her employer's security office and self-reported (1) having brought her personal electronic device into the VTR daily in 2011-2012 and (2) failing to properly secure the VTR on two occasions in early 2015. Ex. 5, Ex. 6, Tr. at 85. Immediately prior to the polygraph, the individual remembered the two times she had unintentionally brought her cell phone into the VTR and self-reported those. *Id.* at 85-86. The individual passed her polygraph examination. *Id.* at 87.

Following her self-disclosure, the individual received a written reprimand from her employer due to the willful nature and extended period of taking her personal electronic device into the VTR and the delay in reporting the two failures to secure the VTR. Ex. 5, Ex. 6, Tr. at 87.

Her employer holds semi-annual forums to increase security awareness and review reporting requirements. The month following her polygraph-inspired disclosures, the individual voluntarily spoke at one of these forums before approximately 75 co-workers and discussed her security lapses and the importance of timely reporting. *Id.* at 18-19. Her senior manager testified that following the individual's talk, the contractor's security office reported the largest number of employees ever coming to inquire about security and disclosure requirements subsequent to a security forum. *Id.* at 20.

Subsequent to her delayed reporting, the individual sought out and completed three non-required on-line training courses related to security. Ex. G at 1-3, Tr. at 91-94.

Subsequent to the individual reporting these violations, she has been very diligent in reporting actual or potential security violations. The individual promptly self-reported two

incidents where she walked into the VTR with her cell phone and, immediately realizing it, exited the VTR and placed the phone outside. *Id.* at 95-99. Both occasions were investigated by her employer's security office and compromise of classified information was ruled out. Ex. A-E. Additionally, she promptly self-reported that she may have included classified information in a voicemail message that she left for a colleague; the security investigation concluded that no classified information was included in the message. Tr. at 94-95.

V. Analysis

I have thoroughly considered the record of this proceeding, including the submissions tendered in this case and the testimony of the witnesses presented at the hearing. In resolving the question of the individual's eligibility for access authorization, I have been guided by the applicable factors prescribed in 10 C.F.R. § 710.7(c)[4] and the Adjudicative Guidelines. After due deliberation, I have determined that the individual's access authorization should be restored. The specific findings that I make in support of this decision are discussed below.

A. Mitigating Evidence

The individual acknowledges that she made errors in bringing her personal electronic device into her secured work area in 2011-2012 and in not promptly self-reporting four more recent unintentional security violations. Tr. at 73, 78-79. Her intentionally bringing a prohibited electronic device into her secured work area, which occurred during a specific period of time approximately four years prior to the hearing, resulted from a combination of frustration from feeling she was being intentionally underutilized by her supervisor and of making her own assessment that such behavior would not create any harm or risk. *Id.* at 72-73. She testified that her judgment with respect to deliberately bringing her electronic device into the VTR was deeply flawed and that she feels shame as a result of that behavior. *Id.* at 74.

The individual argues that her subsequent security violations of failing on two occasions to fully secure her work area and of failing on two occasions to leave her cell phone outside if her secured work area were unintentional, isolated acts. She testified that her decisions to not promptly self-report those occurrences were wrong. *Id.* at 76. Without trying to excuse her actions, she acknowledges being influenced by a workplace culture in which workers tend to (1) assess whether or not a security violation is likely to have caused harm, instead of automatically reporting all incidents, and (2) believe self-reporting is inconvenient and time consuming. *Id.* at 76, 83-84, 114.

---

[4] Those factors include the following: the nature, extent, and seriousness of the conduct, the circumstances surrounding the conduct, to include knowledgeable participation, the frequency and recency of the conduct, the age and maturity at the time of the conduct, the voluntariness of his participation, the absence or presence of rehabilitation or reformation and other pertinent behavioral changes, the motivation for the conduct, the potential for pressure, coercion, exploitation, or duress, the likelihood of continuation or recurrence, and other relevant and material factors.

One of her senior managers affirmed in his testimony that non-reporting at the facility is an issue that management is working to resolve. *Id.* at 36-41. The manager testified that he conducts a semi-annual forum at the facility on security matters and that the individual voluntarily spoke at one of those forums, fully disclosing both her deliberate and her unintentional security violations; her willingness to speak about her experiences has been valuable in influencing others workers. He described her talk as from the "heart." *Id.* at 18-20.

Following her self-reporting in advance of the polygraph examination, the individual sought (and completed) additional training to gain a better understanding of the security issues. Ex. G at 1-3; Tr. at 91-94. The individual also notes that subsequent to her polygraphed-inspired disclosures, she promptly self-reported to her employer's security office two security violations which occurred when she briefly walked into a secured area with her cell phone. *Id.* at 95-97. At the hearing, she articulated the importance of prompt self-reporting of security violations. *Id.* at 90.

Based on the foregoing, the individual argues that she has mitigated the security concerns cited in the Notification Letter.

B. Administrative Judge Evaluation of the Evidence

Criterion G Security Concerns. The individual acknowledges the actions that are alleged in the Notification Letter. *Id.* at 113-116, 1119-120. She violated her employer's security regulations when she walked into the VTR with her personal cell phone on two occasions in 2014 and when she failed to fully secure the VTR on two occasions in 2015.[5] These are significant security violations, but also appear to be infrequent occurrences in the context of the dozens of time each week that the individual enters and exits the VTR. *Id.* at 79-81. *Cf.* Adjudicative Guidelines at Guideline K, ¶ 35(a) (mitigation possible where behavior so infrequent that it does not doubt on the individual's current reliability, trustworthiness, or good judgment). There is no evidence that any classified materials were exposed as a result of these violations. *Tr.* at 27. The failures to alarm the VTR were classified as infractions by her employer and resulted in counseling and a written reprimand.[6] Ex. 5, Ex. 6. Additionally, the individual has voluntarily sought and completed additional on-line training classes on security. Ex. G at 1-3. She has not subsequently failed to fully secure the VTR. *Cf.* Adjudicative Guidelines at Guideline K, ¶ 35(b) (mitigation possible where an individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities).

[5] The Notification Letter also alleges as a Criterion G security concern that the individual intentionally took a prohibited personal electronic device into the VTR in a daily basis in 2011-2012. *See* Ex. 1 at 3. This concern will be discussed in conjunction with the Criterion L security concerns.

[6] The reprimand was also based upon the individual's violation of security regulations for intentionally bringing a prohibited personal electronic device into the VTR on a daily basis in 2011-2012. Ex. 5, Ex. 6.

Entering a closed area with a personal cell phone violates her employer's security policies, but is not reportable to the DOE; her senior manager testified that such events occur weekly at the facility. Ex. B at 1. Tr. at 25. The individual testified as to the precautions she now takes to avoid repeating those lapses. *Id.* at 96. Her co-workers testified that she is diligent in her efforts both to avoid repeating the behavior herself and to remind colleagues entering the VTR to leave their cell phones outside. *Id.* at 62-64, 55-57.

For these reasons, I conclude that such behavior is unlikely to recur and does cast doubt on the individual's current reliability, trustworthiness, or good judgment. *Cf.* Adjudicative Guidelines at Guideline K, ¶ 35(a).

Criterion L Security Concerns. More concerning is that the individual failed to self-report these occurrences to her employer's security office until she was selected for a random security polygraph in April 2015; while the initial security lapses were unintentional, the failures to promptly self-report them were intentional on the part of the individual. In secured working environments, unintentional lapses may occur; however, if they occur, it is important that they be promptly reported so that an accurate assessment can be made with respect to whether any classified or sensitive information was compromised.

Similarly, the individual taking a personal electronic device into the VTR in 2011-2012 was an intentional violation of security regulations. Nonetheless, this occurred during a specific period of time and has not reoccurred in four years. Her manager corroborated her testimony about the frustrations that the individual was experiencing during that period with a supervisor who was transitioning into retirement. Tr. at 31-32. The individual's testimony reflected her genuine remorse over the behavior and her shame at her faulty justification in concluding that her behavior would create no risk since the wireless capability of the device was switched off. *Id.* 73-75. Her testimony also reflected that she has matured in the subsequent years with respect to her ability to manage workplace stress. *Id.* at 117-118. *Cf.* Adjudicative Guidelines at Guideline E, ¶ 17(c), and Guideline K, ¶ 35(a).

In prior cases where Criterion L concerns have been alleged with respect to violating security rules, Administrative Judges have noted that "the overarching concern is … whether the individual will act in the future in a manner that places national security at risk." *See Personnel Security Hearing*, Case. No. PSH-12-0081 (2012) (access authorization restored notwithstanding that the individual delayed disclosing security violations until a polygraph interview and the polygraph examiner subsequently reported the disclosures to the LSO); *Personnel Security Hearing*, Case. No. PSH-12-0083 (2012) (access authorization restored notwithstanding that the individual delayed reporting security violations to the LSO until after two inconclusive polygraph examinations).

Credible testimony of the individual, her senior manager, and co-workers, with respect to the individual's actions subsequent to her polygraph-inspired disclosures, provides important information in assessing whether the individual will act in the future in such a manner as to place national security at risk. Her senior manager testified that twice each year, he conducts forums to sensitize employees on security concerns. Following the

individual's delayed self-reporting of her security violations, she voluntarily agreed to talk at one of the forums about her own violations. Her presentation was described as open and candid, notwithstanding her personal embarrassment over her conduct. Her presentation at the forum occurred months prior to the LSO's commencement of its investigation of her security violations, so this does not appear to be a self-serving attempt to influence the LSO's inquiry. Her senior manager testified that the individual's presentation resulted in the most "robust" response that any of their forums had ever generated, with security reporting their largest number of employees ever asking questions and requesting guidance subsequent to a security forum. Tr. at 20. The manager's testimony acknowledged the difficulty at the facility in terms of a workplace culture where employees assess the risk created by a violation in place of automatically reporting of violations; he noted the value of the individual's efforts in helping management to change that culture.[7] Her co-workers also testified as to the individual's attention to security details and her serving as a mentor to others on security compliance.

The individual also testified as to her "stupidity" in not reporting security events. *Id.* at 74. She clearly articulated that falling into the "no harm/risk" analysis abrogated to herself a decision that she was not qualified to make, that the security professionals in her employer's security office were the ones properly trained to assess whether any information was compromised, and that delayed reporting made it difficult, if not impossible, for them to make an accurate assessment. *Id.* at 76.

Although the individual's actions in 2011-2012 and her failure to promptly report her security violations in 2014 and 2015 reflected unreliable and inappropriate behavior, I conclude that such behavior is unlikely to recur based upon her genuine remorse with respect to her earlier behavior, the steps that she has taken to change her behavior, and her voluntary efforts and candidness in support of management's efforts to change workplace attitudes on security matters. *Cf.* Adjudicative Guidelines at Guideline E, ¶ 17(d). Her changed understanding of the importance of prompt self-reporting is attested to by her having promptly self-reported two subsequent occasions when she walked into the VTR with her personal cell phone and, realizing that she had done so, immediately left the VTR and placed the cell phone outside.

Based upon the foregoing, I find that the individual has sufficiently resolved the Criterion G and Criterion L security concerns.

VI. Conclusion

In the above analysis, I have found that there was sufficient derogatory information in the possession of the DOE that raises serious security concerns under Criterion G and Criterion L. After considering all the relevant information, favorable and unfavorable, in a

[7] The existence of a workplace culture that tolerates non-reporting is attested to be the fact that the second time the individual had failed to fully secure the VTR, it was discovered by her supervisor and he did not report it or instruct her to report. Instead, he left it up to the individual to decide whether or not to report or take it as a "freebie." Tr. at 52-53, 77-78.

comprehensive common-sense manner, including weighing all the testimony and other evidence presented at the hearing, I have found that the individual has brought forth sufficient evidence to resolve the security concerns associated with Criterion G and Criterion L. Accordingly, I have determined that the individual's access authorization should be restored. The parties may seek review of this Decision by an Appeal Panel under the regulations set forth at 10 C.F.R. § 710.28.

Wade M. Boswell
Administrative Judge
Office of Hearings and Appeals

Date: May 19, 2016