*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:	June 3, 2015	)
		) Case No.: PSH-15-0042
		)

Issued: August 27, 2015

Administrative Judge Decision

William M. Schwartz, Administrative Judge:

This Decision concerns the eligibility of XXXXXXXXXXXX (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 discussed below, after carefully considering the record before me in light of the relevant regulations and the Adjudicative Guidelines, I have determined that the individual's access authorization should be restored.

I. Background

The individual works for a DOE contractor in a position that requires that he hold a DOE security clearance. In February 2014, the individual was charged with two counts of Computer Crime and one count of Misdemeanor Conduct in the First Degree. The Local Security Office (LSO) conducted a Personnel Security Interview (PSI) of the individual in May 2014, during which it was not able to resolve the security concerns that these charges raised. On January 28, 2015, the LSO sent a letter (Notification Letter) to the individual advising him that it had reliable information that created a substantial doubt regarding his eligibility to hold a security clearance. In an attachment to the Notification

[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.

Letter, the LSO explained that the derogatory information fell within the purview of one potentially disqualifying criterion set forth in the security regulations at 10 C.F.R. § 710.8, subsection (l) (hereinafter referred to as Criterion L).[2]

Upon his receipt of the Notification Letter, the individual exercised his right under the Part 710 regulations to request an administrative review hearing, and I was appointed the Administrative Judge in the case.[3] At the hearing, the individual's attorneys presented his testimony and that of four other witnesses. In addition to the testimonial evidence, the LSO submitted 11 exhibits into the record numbered 1 through 11, and the individual submitted 17 exhibits, numbered 101 through 117. The exhibits will be cited in this Decision as "Ex." followed by the appropriate numeric designation. The hearing transcript in the case will be cited as "Tr." followed by the relevant page number.

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).

The individual must come forward at the hearing with evidence to convince the DOE that restoring his 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.

---

[2] Criterion L concerns information that indicates that a person has "[e]ngaged in any unusual conduct or is subject to any circumstances which tend to show that the individual is not honest, reliable, or trustworthy. . . . Such conduct or circumstances include, but are not limited to, criminal behavior. . . ." 10 C.F.R. § 710.8(l).

[3] The individual first requested a hearing in February 2015; that request was forwarded to the Office of Hearings and Appeals (OHA) in late March. In his request, the individual stated that court proceedings regarding the criminal charges were scheduled for April 2015. For that reason, OHA determined that the case was not yet ripe for a hearing. Letter from Poli A. Marmolejos, Director, OHA, to individual's attorneys, March 31, 2015. The hearing request was resubmitted to OHA on June 3, 2015, after the presiding judge ruled in the individual's favor.

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 support for its security concerns under Criterion L, the LSO relies on information it obtained from a May 2012 memorandum that placed the individual on administrative leave, the individual's February 2014 indictment, and statements he made during his May 2014 PSI. From that information the LSO determined that the individual had violated the terms of his administrative leave by accessing a police laptop and deleting files and passwords, which formed the basis for the criminal charges. Ex. 1.[4]

I find that there is ample information in the Notification Letter to support the LSO's reliance on Criterion L. Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness, and by its very nature, calls into question a person's ability or willingness to comply with laws, rules, and regulations. *See 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) at Guideline J.

IV. Findings of Fact

The following facts are not disputed. The individual began his career as a police officer in a small town in 2001. By 2004, he had become interested in investigating computer crime. He attended classes and received certifications in computer crime enforcement. Tr. at 84. In 2007, he created and oversaw a high-tech crimes task force that provided assistance to his police department and to law enforcement agencies throughout a large portion of his state. *Id.* at 85. He wrote the policies for use of electronic equipment by both police department and city administration employees. *Id.* at 88. He regularly brought laptop computers and other equipment to his home to repair them and to repurpose them for serving the needs of both his police department and his task force. *Id.* at 62.

On May 16, 2012, the newly appointed acting police chief placed the individual on administrative leave. Though several other people were present when the police chief handed the individual the memorandum that contained the order of administrative leave, none had any experience with the process, and the memorandum was not read aloud or

[4] I note that the LSO did not amend its Notification Letter when it renewed the individual's request for a hearing in June 2015.

signed; nor did the individual read it thoroughly. *Id.* at 96, 98, 100, 102. When the individual asked why he was being placed on administrative leave, no one offered an explanation, including the police chief. *Id.* at 101-02. The memorandum states that the individual was being placed on administrative leave "pending a thorough investigation into issues surrounding the administration and management of the" task force and the withdrawal of one of the participating law enforcement agencies from the task force. Ex. 2 at 10. At the police chief's request, he surrendered his badge, his gun, and a number of passwords for gaining access to various police computer systems, databases and websites. Tr. at 99, 105. The individual then was permitted to take his personal possessions and a copy of the administrative leave memorandum, and was escorted to his home. *Id.* at 105-06. Once at home, he realized that he had additional work-related property there, including a laptop. He notified the department, and a police officer offered to pick up the additional property later that day. *Id.* at 110.

The laptop that the individual turned over to the police department was not its property. It belonged to a neighboring law enforcement agency that had loaned it to the high-tech crimes task force. It was too small to be useful in the forensic work performed by the task force, but the individual was setting it up to assist the task force with video displays at community presentations on internet safety and internet theft prevention. *Id.* at 111, 113, 152-53. As he did with virtually all other computers he repaired or repurposed, he had loaded a stand-alone program called KeePass onto the laptop. KeePass allows the user to store passwords to multiple accounts in one location and access that location with a single password. The list of passwords in the version of KeePass that he loaded onto the laptop concerned personal accounts including financial and medical information as well as personal Microsoft and Adobe accounts that he used to "get those computers set up." *Id.* at 141-46. Before releasing any laptop back into service, he would remove KeePass to eliminate any possibility that his personal passwords might be compromised. *Id.* at 146, 150. On May 16, 2012, before turning the laptop in question over to the police department, he deleted the KeePass program that he had loaded onto it. *Id.* at 114.

The individual maintains that he did not believe he was doing anything improper at the time he removed the KeePass program from the laptop. *Id.* at 150. Even after reading through the administrative leave memorandum the next day, he still did not believe he had done anything that violated the terms of that document, nor has he ever reached that conclusion. *Id.* at 118, 153. He further maintains that he did not remove or alter any other information on the laptop before turning it over to the police department. *Id.* at 151.

The individual attempted, for several weeks, to learn why he had been put on administrative leave, but never received an explanation.[5] He sought new employment, and by July he had been hired by the DOE contractor where he is currently employed, in a different state. He voluntarily resigned from the police department. He explained to

[5] The individual's wife also testified that they never received an explanation of why he was placed on administrative leave. *Id.* at 66-67. They speculate that the action was politically motivated; following the outgoing police chief's retirement announcement, the individual had informed the city administration that he was interested in seeking the position. *Id.* at 79-80. Although this speculation is unsubstantiated, it does offer a motivation for the action as well as a rationale for the employer's refusal to explain the action.

his new employer the circumstances under which he had left the police department, to the extent of his knowledge. *Id.* at 123, 154. As he learned more, he communicated more. *Id.* at 13, 23, 25, 35-36, 52 (testimony of supervisor, employer's security officer, and federal IT oversight).

On August 2, 2012, a few days after starting his new job, the individual learned through a media release that the state police would be conducting the investigation into his actions at the police department. *Id.* at 124. He cooperated fully with the investigation, returning to his home state seven times to participate in it, though he was never told the nature of the allegations. *Id.* at 125-26. In the meanwhile, the LSO granted the individual access authorization in January 2013. *Id.* at 17-18, 132. On February 19, 2014, the individual was indicted on three counts, relating to action he took on May 16, 2012: (1) Felony Computer Crime, for unlawfully, knowingly, and without authorization altering, damaging, or destroying "a computer, computer software, program, documentation, or data contained in such computer or computer system"; (2) Misdemeanor Computer Crime, for unlawfully, knowingly, and without authorization using, accessing, or attempting to access "a computer, computer software, program, documentation, or data contained in such computer or computer system"; and (3) Official Misconduct in the First Degree, for "unlawfully and with intent to obtain a benefit" knowingly performing "an act constituting an unauthorized exercise of official duties" as a public servant. Ex. 2 at 32.

After conducting a hearing in April 2015 regarding the criminal charges described above, the presiding judge dismissed all the charges. In her Order Granting Defendant's Motion to Dismiss, she found the prosecution had failed to preserve the laptop in the state it was in at the time the individual turned it over to the police department and therefore potentially destroyed exculpatory evidence. Ex. 101 at 5. She found that knowledgeable persons at the police department had, on multiple occasions and despite their expertise in handling digital evidence, turned on the computer in a non-forensically sound environment, which might have altered or destroyed data. *Id.* at 6. As a result, the evidence, whether incriminating or exculpatory, was compromised, and she determined that "expert testimony trying to re-create a hard drive through fragments of electronic data to re-create the events of May 16, 2012" was insufficient grounds to sustain the indictment. *Id.* at 7, 11.

The individual's wife, his supervisor, and two co-workers testified regarding his upright and forthcoming character. His supervisor described him as the strongest member of his team, and his co-workers echoed the supervisor's praise of the individual's integrity and reliability, noting his forthrightness in informing them of the embarrassing details surrounding his previous employment. Tr. at 19, 25, 42, 47, 52. Their positive descriptions of his work ethic are reflected in performance evaluations from both his former and current employers and an award he received last year from his current employer. *Id.* at 15-17, 19, 47, 50; Exs. 110-115.

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) and the Adjudicative Guidelines. After due deliberation, I have determined that the individual's access authorization should be restored. I find that restoring the individual's DOE security clearance will not endanger the common defense and security and is clearly consistent with the national interest. 10 C.F.R. § 710.27(a). The specific findings that I make in support of this decision are discussed below.

I find that the individual has no cognizable record of criminal activity. I reach this finding on the basis of the individual's testimony and the absence in the Notification Letter of criminal charges prior to the 2014 indictment. Tr. at 155-56; Ex. 1. As for the facts underlying the 2014 indictment, the individual's testimony, supplemented by that of the other witnesses and the exhibits submitted in this proceeding, paints a consistent and uncontroverted portrait of an upright individual. The individual was a dedicated, hard-working employee who developed a specialized and much-needed expertise in high-tech crime law enforcement. Placed on administrative leave for an unspecified reason, he turned over all his business property to his employer, as requested. Among that property was a laptop he was in the process of rebuilding, which contained personal passwords stored in a single file, KeePass. He deleted that file before turning in the laptop to the police department for two reasons: (1) it was not business property, and (2) not deleting it would compromise the privacy of his family. Moreover, deleting that file was his standard practice; before placing any computer back in service, he always deleted the KeePass file.

On the basis of the evidence in this proceeding, including the testimony, the exhibits, and the disposition of the criminal charges in state court, the offenses listed in the Notification Letter are unsubstantiated. The Adjudicative Guidelines enumerate factors that can mitigate security concerns raised by an individual's behavior or circumstances. Guideline J, which addresses criminal activity, sets forth a number of circumstances that can mitigate security concerns based on such activity, including "evidence that the person did not commit the offense." Adjudicative Guidelines at ¶ 32(c). I find that the criminal charges the individual faced do not cast doubt on his reliability, trustworthiness, or good judgment. Consequently, I find that the individual has resolved the LSO's security concerns.

VI. Conclusion

In the above analysis, I have found that there was sufficient derogatory information in the possession of the DOE to raise serious security concerns under Criterion L. After considering all the relevant information, favorable and unfavorable, in a 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 this criterion. I therefore find that restoring the individual's access authorization will not endanger the common defense and is clearly consistent with the national interest. Accordingly, I have determined that the individual's access authorization should be restored.

William M. Schwartz
Administrative Judge
Office of Hearings and Appeals

Date: August 27, 2015