*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-16-0007
		)

Issued : June 21, 2016

Administrative Judge Decision

Wade M. Boswell, Administrative Judge:

This Decision concerns the eligibility of XXXXXXXXXXXXX (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 not be restored.

I. Background

The individual is employed by the DOE in a position that requires her to hold DOE access authorization. In January 2015, one of her co-workers, who was also a holder of DOE access authorization, was arrested. Local police sent an e-mail to their liaison for the DOE site reporting information on the arrest. This e-mail and the co-worker's official arrest report were subsequently transmitted to multiple locations within the DOE complex using a digital scanner; the scanner did not identify the sender of the information and the transmitted information (which included, *inter alia*, the co-worker's arrest information and his date of birth) was not encrypted. These transmissions triggered an internal DOE investigation, which identified the individual as the person that originated these transmissions. *See* Exhibit 5. The individual acknowledges having done so.

[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.

The individual was interviewed as part of the internal investigation and, at the commencement of the interview, she signed an agreement not to disclose the content of the investigation. Immediately after leaving the interview, the individual telephoned another DOE employee and discussed the investigation. *See* Exhibit 5.

Due to concerns about the individual's conduct which was documented during the internal investigation, the Local Security Office (LSO) conducted a personnel security interview (PSI) with the individual in August 2015. *See* Exhibit 6. Since the PSI did not resolve these concerns, 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 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] *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 the testimony of one witness, a DOE personnel security specialist. The individual introduced 28 lettered exhibits (Exhibits A – CC)[3] 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.[4]

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)

[2] See Section III below.

[3] At the request of the individual, a document initially presented by the individual and labelled as Exhibit R was stricken from the record. The individual's subsequent submissions were not re-lettered; therefore, the record contains no Exhibit R. Transcript at 9.

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

("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 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 one criterion as the basis for suspending the individual's security clearance: Criterion L. 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 reflecting questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations raises questions about an "individual's reliability, trustworthiness and ability to protect classified information." *See* Guideline E 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 L, the LSO alleges, *inter alia*, that: (1) the individual removed an e-mail about her co-worker's arrest from her supervisor's office, without his permission, and transmitted copies of the e-mail, unencrypted, to both her government and personal e-mail accounts using a government digital scanner; (2) the individual requested a DOE contractor employee to provide her with the fax number of the local Rotary Club and, thereafter, attempted to transmit her co-worker's arrest information to the Rotary Club using government equipment, while on duty; (3) the individual, while using a government computer and while on duty, entered the arrested co-worker's name and date of birth on a website in order to ascertain any crimes with which he may have been charged and any fines he may have paid; (4) the individual transmitted copies,

unencrypted, of the official police report of her co-worker's arrest to two DOE offices and several DOE employees who did not have a "need to know" about the arrest; and (5) the individual breached a non-disclosure agreement she signed as part of an internal DOE investigation by discussing the investigation with another co-worker. Ex. 1 at 1-2.

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

IV. Findings of Fact and 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)[5] and the Adjudicative Guidelines. After due deliberation, I have determined that the individual's access authorization should not be restored. I cannot 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.

A. Mitigating Evidence

At the hearing, the individual's testimony was candid and direct. In mitigation of the security concerns described in the Notification Letter, the individual presented much detail on certain factual matters where she believed the LSO had erred, as well as arguments against certain conclusions that the LSO had reached. However, many of the distinctions argued are, ultimately, not dispositive of the security concerns before me. For example, the Notification Letter refers to the individual having instructed a DOE contractor to "perform an internet search" (Ex. 1 at 1) to obtain certain information and, while the DOE contractor may or may not have performed an internet search to get the information, the individual argues that she did not request that an internet search be conducted. Tr. at 178, 199. Consistent with the individual's contention is an e-mail from the individual to the DOE contractor instructing the contractor to "call" (Ex. 5 at 80) to get certain information. Whichever facts are correct (and, in this case, I believe those advocated by the individual are correct), the underlying security concern is unaffected: Did the individual use government time and resources (whether it was a telephone or a computer)[6] for non-governmental purposes in such a manner as to evidence doubt about her reliability, trustworthiness, honesty or judgment?

---

[5] 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.

[6] Government resources in this instance also includes the individual seeking the assistance of a DOE contractor employee. *See* DOE Order 203.1 at ¶ 4.f(2).

In those instances where the individual has contested the LSO's facts or conclusions, I have carefully considered the totality of the individual's testimony, the entirety of the record, and the arguments presented by both the individual and the LSO in my evaluation and in reaching the findings of facts set forth below.

B. Administrative Judge Evaluation of the Evidence and Findings of Fact: Criterion L Security Concerns

Most of the facts cited in the Notification Letter are not contested and, as noted above, many of those facts that are contested relate to distinctions that are, ultimately, not significant to the adjudication of the security concerns at issue. Similarly, the individual and the LSO focused much attention on the nature and scope of personally identifiable information (PII) and the duties of DOE personnel with respect to PII, and, while those issues are important and thought provoking,[7] they obscure the fundamental national security concerns presented in this case.

The Notification Letter sets forth four factual bases for the Criterion L security concerns, each of which will be analyzed separately.

E-mail from Local Police Department. A DOE employee was arrested by local police and, during the arrest, he identified himself as a DOE employee who had a security clearance. A police sergeant forwarded information about the arrest (including the name of the arrested employee, the details of the arrest and alleged criminal behavior, and the employee's birthdate) in an e-mail to the chief of the local police department; the police chief, in turn, forwarded that e-mail with a cover note (collectively, Police E-mail) to his federal liaison (Liaison or Federal Liaison). Ex. 5 at 42-43. The Federal Liaison contacted a manager of the local DOE site and advised him of the arrest. The following day, the DOE

[7] DOE Order 206.1 refers to the directives of the Office of Management and Budget in defining PII and the responsibilities of DOE personnel with respect to PII. PII includes a person's criminal history and the date of birth. DOE Order 206.1 at ¶ 4.a(1). In this case, the arrested co-worker's arrest information and date of birth were both included in the documents that the individual disseminated. The individual's argument that information of a single arrest does not constitute a "criminal history" under DOE Order 206.1 is without legal merit and ignores the clear meaning and intent of the DOE Order. Her arguments that only information marked as protected or included in a "systems of record" noticed in the Federal Register is entitled to protection under DOE Order 206.1 evidences a fundamental misreading of the DOE Order and the distinctions contained therein with respect to PII covered by the Privacy Act and PII not covered by the Privacy Act. Her arguments that, since arrest records are releasable under her state's Freedom of Information Act and are deemed public information by her state, arrest records and information originating in her state are not subject to protection under DOE Order 206.1 ignores (1) the primacy of a DOE Order with respect to the protection by DOE of information in its possession and (2) the duty of care required by the DOE Order with respect to certain personal information notwithstanding that that information may be publicly available elsewhere (e.g., a person's date of birth or mother's maiden name). However, even if I had accepted all of the individual's arguments with respect to PII or had found that she mitigated all of the security concerns with respect to her mishandling of PII, she would have failed to have resolved the security concerns which are analyzed in this section of the Decision under the subheadings of: E-mail from Local Police Department; Interaction with DOE Contractor Employee; Dissemination of Official Police Record; and Breach of Non-Disclosure Agreement.

manager went to the Liaison's office and received a printed copy of the Police E-mail. Tr. at 140-141.

The DOE manager showed the individual, who he supervised, the Police E-mail. The individual and the arrested employee had an adverse relationship and, based upon information submitted by the individual into the record, the arrested employee had been named by the individual in complaints[8] that she had filed with the DOE Inspector General (IG). Ex. U at 1, 4, 6, 8; Tr. at 10-11. The individual testified that she believed that DOE management had been "covering up" behavior by the arrested employee "for years" and that she believed management would not take appropriate actions with respect to his arrest. *Id*. at 155-156, 165, 193.

On the same day that the DOE manager showed the Police E-mail to the individual, the individual entered the manager's office while he was at lunch and retrieved the Police E-Mail. *Id.* at 164, 175, 192-193. Before returning it, she scanned the Police E-mail on a digital sender and e-mailed it to herself at both her government and personal e-mail accounts (as well e-mailing it to other locations). *Id.* at 175, 192-193. She acknowledges that she did not have her supervisor's permission to access or send the Police E-mail, although she also states that she does not believe she needed his permission to do so. *Id.* at 175-176, 195. She justifies her actions based upon her needing the Police E-mail in order to report her co-worker's arrest to the DOE and upon the fact that arrest records are public information in their jurisdiction. *Id.* at 135, 175, 193.

While the individual is correct that arrest records are public documents in their jurisdiction, the Police E-mail is not an arrest record. It is an e-mail from the chief of the local police department to his Federal Liaison, which was provided to the DOE manager for official government purposes.[9] Ex. 5 at 42-43; Tr. at 138-140. The Police E-mail, once in the possession of the DOE manager, was a federal government document. The individual had no authority to take possession of the document or to convert the document to one that she could use personally, which she accomplished by e-mailing it her own e-mail accounts. Such conduct, on its face, demonstrates unreliability and untrustworthiness and falls clearly within the security concerns described by Criterion L. *See* 10 C.F.R. § 710.8(l).

The individual attempts to justify her behavior by pointing to the obligations of those holding access authorization to report certain events, whether those events relate to themselves or to another holder of access authorization. In mitigation of her conduct, she argues that, since she holds access authorization, she is required to report the arrest of another holder of access authorization. Tr. at 156. Further, she argues that, since she had

[8] Based on at least one exhibit submitted by the individual, actions of the arrested co-worker are also at issue in a complaint filed by the individual with the U.S. Equal Opportunity Commission. *See* Ex. O at 3.

[9] The Federal Liaison, who was the addressee of the Police E-mail, testified at the hearing at the request of the individual. In his testimony, he noted that under the state laws of their jurisdiction the individual's official arrest record was publicly available (without redaction), but that the Police E-mail would not be a publicly available document under their state laws even though it included information about an arrest. Tr. at 138-140.

concluded that her management had ignored past misconduct of the arrested employee, she reasonably believed management would do so in the case of his arrest as well. *Id.* at 155-156, 165, 193. Essentially, she suggests that she needed to collect evidence of the arrest. *Id.* at 182. In making this argument, the individual dangerously inflates the obligations that a holder of access authorization has to report the conduct of others. The obligation is to report known information, not to investigate. The individual testified that she orally reported the arrest of her co-worker to her facility's security officer, who was an appropriate authority for her to report the information. *Id.* at 205-206. Having reported the information to an appropriate authority within her organization, she had fulfilled her reporting obligation. Once the information is appropriately reported within the DOE organization, the responsibility is then upon the DOE security organization, which is staffed with properly trained personnel, to evaluate the information and, if necessary, investigate it. If the individual is sincere in her argument that she was merely trying to perform her own obligations as a holder of access authorization, she would have disengaged after reporting the arrest information and allowed the DOE security organization to perform its function. Further, the individual presented no viable explanation as to how properly reporting her co-worker's arrest justified her assuming ownership of a federal government document (i.e., the Police E-mail), which she did by sending it to her personal e-mail account. Such behavior reflects poor judgment and dishonesty and breached her inherent fiduciary obligations as an employee of the federal government. *Cf.* Adjudicative Guidelines at Guideline E, ¶ 16(d)(1).

Based on the foregoing, I find that the individual has not resolved the security concerns associated with Criterion L arising from actions with respect to the Police E-mail.

Interaction with DOE Contractor Employee. The day after the individual learned of her co-worker's arrest, the individual requested a DOE contractor employee to provide her with the fax number of the local Rotary Club; the individual then attempted to fax the Police E-mail to the local Rotary Club using a federal government scanner. Tr. at 166-167, 199, 203. Due to a technical error, the fax failed. *Id.* at 199.

Other than a general comment that she thought people needed to know about her co-worker's arrest and felt that it was appropriate to disseminate information about the arrest since it was public information, the individual did not provide (nor could she) any viable justification for her actions.[10] *Id.* at 200. But for a technical error, she would have disseminated the Police E-mail to a non-government entity. She had no authority to possess the Police E-mail, as noted above, and, therefore, had no authority to disseminate it. There is no possible argument that the individual had a duty as a holder of access authorization to report information about other holders of access authorization to non-federal entities. Federal employees are required to use government time and resources[11] for federal

[10] At the hearing, the individual acknowledged that this had been a bad choice and that, in retrospect, she was glad that the transmission had failed. Tr. at 200-201.

[11] Federal resources, in this case, include both the time of the federal contractor and the government-owned equipment. *Cf.* DOE Order 203.1 (inappropriate uses of government resources include seeking help from Government employees or contractor personnel in pursuit of personal projects).

purposes; there was no federal purpose in reporting the arrest of a DOE employee to the local Rotary Club. *See* DOE Order 203.1. This behavior is more akin to vigilantism than to the prudence expected of federal workers while on duty, on government premises and using federal equipment, and demonstrates poor judgment, unreliability and untrustworthiness. *See* 10 C.F.R. § 710.8(l).

Although the individual acknowledged that it was a lapse of judgment for her to attempt to disseminate information about her co-worker's arrest to the local Rotary Club, she attempts to deflect the responsibility for this behavior by stating that the idea to disseminate the arrest information to the local Rotary Club originated with the contractor. Tr. at 166. However, faxing a non-public document containing a co-worker's arrest information outside of the federal government (whether or not the transmission was successful) on government time, using government equipment, was a monumental lapse in judgment by a mature professional with over three decades of experience and any suggestion by the individual that she could have been influenced into committing such inappropriate behavior further demonstrates unreliability and untrustworthiness. *See* 10 C.F.R. § 710.8(l). The presentation by the individual of this argument in mitigation of the Criterion L security concerns does not mitigate the concerns, but reinforces them.

In a second interaction with the contractor, the individual admitted to instructing the contractor to access a website to look-up the co-worker's arrest record. Tr. at 202. Subsequently, the individual entered the co-worker's name, date of birth and arrest report number on a website provided to her by the contractor in order to ascertain whether there were any criminal charges filed against their co-worker and whether any fines had been paid by their co-worker. *Id.* at 202-203. This was also done while on government time and using a government computer. *Id.* at 203. The individual justifies this behavior based on her needing to know the details and status of her co-worker's arrest because she thought that those factors would influence what, if any, actions her management might take with respect to the individual's arrest. Ex. 6 at 65; Tr. at 202-203. However, as noted above, investigating information about one's co-workers (even if it may be related to security concerns) is the jurisdiction of management and personnel security, not self-assigned co-workers. *Cf.* Adjudicative Guidelines at Guideline E, ¶ 16(d)(4).

At times, the individual had functioned as her facility's security representative; however, she acknowledged that, even in that capacity, her obligation would have been limited to reporting the information she received to higher management, not independently investigating it. Tr. at 204-206. While information that she and the contractor sought to discover in their internet search may have been of some personal interest to them, it was not in fulfillment of the individual's government responsibilities and, therefore, was an inappropriate use of government time and resources and reflected poor judgment, unreliability and untrustworthiness. *Cf.* Adjudicative Guidelines at Guideline E, ¶ 16(d)(4).

Based on the foregoing, I find that the individual has not resolved the security concerns associated with Criterion L arising from her interactions with a DOE contractor employee with respect to their arrested co-worker.

Dissemination of Official Police Report. Approximately four days after first learning of her co-worker's arrest, the individual drove to the local police department and obtained the official police report of her co-worker's arrest. Tr. at 176, 196. The individual credibly established that the report was available to any citizen of their state requesting it and, under state law, information such as an arrestee's name, address and birthdate is not redacted. *Id.* at 115-119, 124-126. Local law enforcement officers corroborated this practice. *Id.* at 125. Therefore, the individual had the right to obtain and possess the police report for her own personal use; however, the individual conflates her personal right to possess the police report with her right to distribute it within DOE using government-owned equipment and while on government time.

Subsequent to receiving a copy of the official police report on her co-worker's arrest, the individual transmitted it, unencrypted, by use of a government scanner to at least four of her co-workers. *Id.* at 197. She disagrees with the LSO's judgment that those co-workers did not have a "need to know" about the arrest of one of their colleagues. She argues that "need to know" is relevant to classified documents and that the arrest record is not classified or labeled in any way to prohibit its distribution. *Id.* at 197-198. She also argues that the recipients of her transmission needed to know about the behavior of the co-worker which led to his arrest and to know the "kind of person that he was." *Id.* at 177, 198-199. However, the individual makes no viable arguments to connect her judgment that certain co-workers should know about their co-worker's arrest with the performance of her duties as a federal government employee. She attempts to connect her actions to her obligation as an access authorization holder's obligation to report certain security events relating to other holders of access authorization. *Id.* at 156. However, this ignores that the reporting obligation is a narrow obligation and that she fulfilled it several days earlier when she notified her facility's security representative of the arrest; any concern that her initial reporting had been insufficient or would be "covered-up" should have been resolved when she transmitted the official police report (contemporaneously with the transmission to her four co-workers) to a DOE personnel security office and the arrested employee's upper level manager. *Id.* at 176, 196. The individual introduced no viable information into the record that substantiated any official need of her co-workers to know of the arrest of their other co-worker.[12] Taking it upon herself to personally decide who within the DOE complex should be informed about her co-worker's arrest usurps authority that properly belonged to DOE security and DOE management. *Cf.* Adjudicative Guidelines at Guideline E, ¶ 16(d)(2) (disruptive or other inappropriate behavior in the workplace).

As noted above, I find no connection between the individual's transmission of the police report to co-workers with the performance of her official duties. Use of government resources (e.g., the government scanner used to transmit the police report) is limited to the

[12] The individual testified that some of her co-workers to whom she transmitted the information were witnesses to the events described in her complaint to the IG and, therefore, needed to know about the arrest. Tr. at 160. This argument ignores that the co-worker's arrest was not related to the substance of her IG complaint (other than in the broadest sense that both related to the co-worker's "ethics") and that the individual had made the IG aware of the co-worker's arrest by transmitting to the IG both the Police E-Mail and the official police report (on separate occasions). *Id.* at 176.

performance of official government functions. As such, use of government equipment by the individual to transmit her co-worker's police report to other co-workers demonstrates poor judgment and lack of reliability.

The individual argues that government employees are permitted *de minimis* personal use of government owned equipment (Ex. 2 at 2; Ex. BB at 10); however, *de minimis* personal use does not permit inappropriate use of government equipment. The co-worker's name, arrest information,[13] and date of birth, which constitutes PII under DOE orders, were in the documents transmitted by the individual. Ex. 5 at 41-49. *See* DOE Order 206.1 at ¶ 4.a(1). A DOE employee in the performance of their government duties could not have digitally transmitted such documents to people of their own choosing nor could he or she have transmitted such documents (even in the course of legitimate federal activates) without encryption or other proper protection. *See* DOE Order 206.1. A DOE employee cannot engage in such activities as a personal matter while using government time and equipment and then claim protection of the workplace rules that permit *de minimis* personal use of government equipment. *See* DOE Order 203.1.

Based on the foregoing, I find that the individual has not resolved the security concerns associated with Criterion L arising from actions with respect to dissemination of the official police report of her co-worker's arrest.

Breach of Non-Disclosure Agreement. As noted above, the individual distributed, without encryption, the official police report of her co-worker's arrest within the DOE complex via a digital scanner. This scanner did not identify the sender of the report, so the report appeared to those receiving it as being sent anonymously. This triggered an internal DOE investigation. *See* Ex. 5 at 2. The individual interprets the internal investigation as unfairly targeting her and as further evidence that management sought to protect her arrested co-worker, ignoring the fundamental role she played by "anonymously" sending one or both of the Police E-mail and the official police report (each containing information about a DOE employee's criminal arrest and other personal information, such as his date of birth) to at least seven locations in the DOE complex. Failure to anticipate the reaction to her "anonymous" distribution of her co-worker's arrest information and other PII demonstrates poor judgment. *Cf*. Adjudicative Guidelines at Guideline E, ¶ 16(d)(2) (disruptive or other inappropriate behavior in the workplace).

Those conducting the internal investigation, interviewed the individual and, at the commencement of that interview, the individual signed a non-disclosure form agreeing that she would not disclose the content of the investigation to anyone. Ex. 5 at 100. According to the individual, the investigators were keen to discover certain details about the dissemination of information about the co-worker's arrest and she was uncertain about whether she had sent the Police E-mail to a certain person. Tr. at 184. When the individual left the interview, she went to her car and, within fifteen to twenty minutes of the

[13] DOE Order 206.1 describes PII as including information about an individual's "criminal history." The individual argues that information about a single arrest does not constitute a "criminal history." Tr. at 187-191. This argument ignores the plain intent and language of DOE Order 206.1 and is without legal merit.

conclusion of the interview, called the other person and discussed the investigation. *Id.* at 185. The individual argues that she did so only in order to obtain information sought by the investigators and to further the investigation and that she had not discussed the "details" of the investigation. *Id.* At the hearing, she focused upon telephone records which evidenced that her conversation with this other person had been a four-minute conversation. *Id.*

Understanding confidentiality requirements and maintaining confidentiality are paramount to the protection of national security. In this instance, the individual beached confidentiality within minutes of exiting an interview during which she had agreed, in writing, to maintain confidentiality. Similar to her arguments discussed above in which she posited her obligation to investigate the arrest of her co-worker, the individual argues with respect to the internal investigation that she needed to speak to this other person in order to obtain information sought by the investigators. *Id.* at 184. Again, she is attempting to conduct her own investigation, as opposed to providing the information known to her and allowing those tasked with the investigation to perform their responsibilities. Failure to maintain confidentiality could endanger the success of an investigation.

While I accept her argument that she was, in good faith, trying to assist the investigators by gathering information that she did not remember, that she would do so demonstrates a basic misunderstanding of fundamental security protocols. Not only did she breach confidentiality, but she seemed not to have recognized that she had done so until six months later when she was questioned about it by the LSO during the PSI. Ex. 6 at 94-97. While she does not deny discussing the internal investigation in the telephone call she had with the other person immediately after leaving the interview, she attempts to minimize the magnitude of her breached by focusing on the call being only four minutes in length. Tr. at 185. Her written non-disclosure agreement was to *not disclose* the content of the investigation; it was not to limit her disclosures to what could be relayed in four minutes. To argue that a security concern arising from her breach of a non-disclosure agreement is mitigated by the brevity of her breaching communication demonstrates a fundamental lack of understanding of security requirements and, making such an argument, exacerbates security concerns about the individual's judgement and reliability. *See* 10 C.F.R. § 710.8(l).

Based on the foregoing, I find that the individual has not resolved the security concerns associated with Criterion L arising from her breach of the non-disclosure agreement that she signed in conjunction with the internal DOE investigation.

Whole-Person Concept. The individual argues that the actions cited in the Notification Letter occurred over the course of a brief period of time, which followed an extreme period of distress for her in the workplace which she seems to attribute to her arrested co-worker. In light of her otherwise unblemished career of over thirty years, she argues her behavior is mitigated by reference to the "whole-person" concept incorporated in Part 710 and the Adjudicative Guidelines. Ex. BB; Tr. at 217.

While I agree that the events noted in the Notification Letter all occurred within a period of a couple weeks, the egregiousness of the individual's behavior in the context in which it occurred supports a whole-person assessment of questionable judgment and an inability to properly safeguard information on the part of the individual. *See* Adjudicative Guidelines at Guideline E at 16 ¶ d(1), (2) and (3).

For the reasons discussed above, I find the individual has not resolved the security concerns associated with Criterion L.

V. 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 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 not brought forth sufficient evidence to resolve the security concerns associated with Criterion L. Accordingly, I have determined that the individual's access authorization should not 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: June 21, 2016