* 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 6, 2012 | ) | |
| | ) | Case No.: PSH-12-0071 |
| | ) | |

Issued: October 22, 2012

## Hearing Officer Decision

Steven L. Fine, Hearing Officer:

This Decision concerns the eligibility of XXX XXXXXXX (hereinafter referred to as "the Individual") to maintain a security clearance under the regulations set forth at 10 C.F.R. Part 710, entitled "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material." For the reasons set forth below, I conclude that the Individual's security clearance should not be restored.

## I. BACKGROUND

In 2008, the DOE granted the Individual a security clearance after he resolved derogatory information concerning his three extramarital affairs, and provided assurances that a civil lawsuit that was pending against him at the time was frivolous and devoid of merit.

In early 2012, the Individual informed a Local Security Office (LSO) that criminal charges had been filed against him for "Computer Crime and Grand Theft." DOE Exhibit 2 at 24-25. The LSO conducted a Personnel Security Interview (PSI) of the Individual on March 14, 2012, to discuss these charges. At that time, the Individual revealed that a trial had been conducted in the civil lawsuit and that a jury had awarded a $2.1 million judgment against him and two other defendants, for Breach of Fiduciary Duty, violation of a state Trade Secrets Act, and Civil Conspiracy.

Unable to resolve the security concerns relating to the civil lawsuit judgment or the criminal charges, the LSO initiated administrative review proceedings by issuing a letter (Notification Letter) advising the Individual that it possessed reliable information that created a substantial doubt regarding his eligibility to hold a security clearance. In the Notification Letter, the LSO

set forth the derogatory information at issue and advised that the derogatory information fell within the purview of potentially disqualifying criteria set forth in the security regulations at 10 C.F.R. § 710.8, subsection (l).[1]

The Notification Letter informed the Individual that he was entitled to a Hearing before a Hearing Officer in order to resolve the substantial doubt regarding his eligibility for access authorization. The Individual requested a Hearing, and the LSO forwarded his request to the Office of Hearings and Appeals (OHA). The Director of OHA appointed me as the Hearing Officer in this matter on June 11, 2012.

At the Hearing I convened pursuant to 10 C.F.R. § 710.25(e) and (g), I took testimony from the Individual, four colleagues, his supervisor, his clergyperson, and a DOE Personnel Security Specialist. *See* Transcript of Hearing, Case No. PSH-12-0071 (hereinafter cited as "Tr."). The LSO submitted six exhibits, marked as DOE Exhibits 1 through 6, and the Individual submitted 17 exhibits, marked as Individual's Exhibits 1 through 17.

## II. STANDARD OF REVIEW

The Hearing Officer's role in this proceeding is to evaluate the evidence presented by the agency and the Individual and to render a decision based on that evidence. *See* 10 C.F.R. § 710.27(a). The regulations state that "[t]he decision as to access authorization is a comprehensive, common-sense judgment, made after consideration of all relevant information, favorable or unfavorable, as to whether the granting or continuation of 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 have considered the following factors in rendering this decision: the nature, extent, and seriousness of the conduct; the circumstances surrounding the conduct, including knowledgeable participation; the frequency and recency of the conduct; the Individual's age and maturity at the time of the conduct; the voluntariness of the Individual's 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. *See* 10 C.F.R. §§ 710.7(c), 710.27(a). The discussion below reflects my application of these factors to the testimony and exhibits presented by both sides in this case.

---

[1] Specifically, the Notification Letter alleges that the Individual has:

> Engaged in any unusual conduct or is subject to any circumstances which tend to show that the individual is not honest, reliable, or trustworthy; or which furnishes reason to believe that the individual may be subject to pressure, coercion, exploitation, or duress which may cause the individual to act contrary to the best interests of the national security. Such conduct or circumstances include, but are not limited to, criminal behavior, a pattern of financial irresponsibility, conflicting allegiances, or violation of any commitment or promise upon which DOE previously relied to favorably resolve an issue of access authorization eligibility.

10 C.F. R. § 710.8(l)

## III. FINDINGS OF FACT

The facts in this case are complicated. Where appropriate, I rely on findings rendered in judicial proceedings as the foundation for my findings of fact.

Between 2000 and 2007, the Individual worked as a member of Employer A's management team. Employer A experienced a change in ownership, and the Individual found himself working for Employer A's new owner (Owner A) with whom he had a strained relationship. Tr. at 115. A firm from a neighboring state, Employer B, sought to open a new facility in Employer A's state and compete with Employer A. On August 3, 2007, the Individual, along with two other management level employees of Employer A (Manager #1 and Manager #2) met with Employer B's Chief Executive Officer (CEO) and Chief Financial Officer (CFO), and began discussions which ultimately resulted in their accepting offers of employment with Employer B. DOE Exhibit 6 at 9; Individual's Exhibit 1 at 3-4. The Individual terminated his employment at Employer A on September 21, 2007, and then began working for Employer B. DOE Exhibit 6 at 3.

### The External Hard Drive

One to two weeks before he left Employer A, the Individual backed up the contents of a laptop computer (the Laptop), owned by Employer A, onto a portable external hard drive that he had purchased. DOE Exhibit 2 at 8-9, 16-17; Tr. at 117. At approximately the same time, Manager #1 also copied the contents of his Employer A-owned computer to another external hard drive.[2] In his court testimony, the Individual admitted that he knew that the external hard drive contained Employer A's information, including quality manuals, vendor information, customer information, when he took it.[3] DOE Exhibit 3 at 248, 264. However, the Individual denied knowing whether the information he took was confidential or proprietary. *Id.* at 248-249.

When he left Employer A to work at Employer B, the Individual brought the external hard drive home. DOE Exhibit 2 at 15; Tr. at 117. After the civil suit was filed against the Individual, Manager #1, and Employer B, Employer B's Human Resource Department informed the Individual and Manager #1 that the external hard drives were subject to a discovery request filed by the plaintiff, Employer A, and directed them to turn the external hard drives over to legal counsel representing the three defendants. Individual's Exhibit 1 at 5. The Individual provided the legal counsel with the external hard drive. DOE Exhibit 3 at 267, Tr. at 117, 128-131.

---

[2] At the civil trial, Manager #1 testified that he had informed the Individual of his intention to download the information on the hard drive of the computer issued to him by Employer A to an external hard drive. DOE Exhibit 2 at 13. The Individual testified, at the civil trial, that he recalled hearing Manager #1's testimony that they had discussed downloading information from Employer A's computers, before Manager #1 downloaded information from Employer A's computer to an external hard drive. The Individual, however, did not recall that conversation. DOE Exhibit 3 at 243-244. The jury's finding that he was part of a civil conspiracy was apparently based upon this conversation. DOE Exhibit 2 at 13.

[3] The trial court described the information copied to the external hard drives as: "(1) [Employer A's] customer lists; (2) [Employer A's] jobs; (3) information regarding how [Employer A] estimates and prices its jobs, including [Employer A's] costs and mark-up; (4) [Employer A's] vendors; (5) [Employer A's] Quality Assurance Program; and (6) customers and customer contact information." Individual's Exhibit 1 at 5.

**The August 20, 2012, Email**

On August 20, 2007, while he was employed by Employer A, the Individual wrote an email to Employer B's CEO, which he also circulated to Manager #1, Manager #2, and Employer B's CFO. DOE Exhibit 2 at 18. In this email, the Individual states, in pertinent part:

> Attached is a brief listing of personnel and salaries from the [XXX] Department. My hopes would be to aquire [sic] each of these individuals as soon as the decision is made to move ahead. I am in complete agreement with [Manager #2] and [Manager #1] in respect to making this happen as quickly and smoothly as possible for all parties involved. I look forward to our next meeting and discussions. I have also begun some searching for a possible location and will update you with what we find.

Individual's Exhibit 3 at 1. The Individual did not provide specific names of employees, but instead, provided position descriptions, salary ranges, and skill descriptions, that mirrored employees at Employer A. *Id.* at 2. During his testimony before the trial court during the civil action, the Individual admitted that the email list described specific employees of Employer A that he sought to hire at Employer B. DOE Exhibit 3 at 275-280. At the Hearing however, the Individual described this list as a "wish list" of positions he wished to create once he joined Employer B, rather than a list of specific individuals that he sought to hire, and testified that these salary ranges came from his experience at Employer A and from his research at "Salary.com." Tr. at 142.

**The Non-Disclosure Agreement**

The State Court with jurisdiction over the civil lawsuit at issue in the present decision (the State Court) held, in deciding interlocutory motions, that the Individual "had a nondisclosure agreement with [Employer A] whereby he promised not to disclose [Employer A's] confidential information to any person, and that he would surrender to [Employer A] 'all papers and records of any kind' related to the business and affairs of [Employer A] or any of [Employer A's] customers upon termination of his employment." Individual's Exhibit 1 at 2-3. However, the State Court further found that this non-disclosure agreement was not enforceable under the applicable state law. Individual's Exhibit 1 at 13.

The State Court held a civil trial in December 2011, in which a jury found in favor of Employer A and assessed damages of 2.1 million dollars against the Individual, Manager #1, and Employer B. DOE Exhibit 2 at 4; DOE Exhibit 4 at 19. The jury found the Individual liable for Breach of a State Trade Secrets Act, Civil Conspiracy, and Breach of Fiduciary Duty. DOE Exhibit 2 at 5.

During his March 14, 2012, PSI, the Individual reported that criminal charges had been filed against him for "Computer Crime and Grand Theft." DOE Exhibit 2 at 24-25. The Individual claimed that he did not know that his actions might be illegal and expressed his intent to contest the criminal charges. *Id.* at 32-34. Nevertheless, the Individual stated that he still thought that copying the information on the laptop and taking that information when he went to work for a

competitor was "very wise."[4] *Id.* at 14. The Individual denied that he had taken the information for the benefit of Employer B, or in order to harm Employer A. *Id.* at 14, 45. The criminal charges were eventually dismissed, without prejudice. Tr. at 146-147, 166-167.

## IV. DEROGATORY INFORMATION AND SECURITY CONCERNS

The record shows that the Individual, violated his previous employer's rules and regulations, by copying the contents of his employer's hard drive, which included proprietary and confidential information, to his own external hard drive.[5] These actions demonstrate that the Individual misappropriated that information. The record also shows that a civil court has found that, while he was employed by Employer A, the Individual supplied Employer B with proprietary and confidential information meant to facilitate Employer B's hiring away of key employees from Employer A.

"Untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information" are among those "Conditions that could raise a security concern and may be disqualifying." *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) Guideline E at ¶ 15, ¶16(d)(1). Moreover, the facts cited above show that the Individual has engaged in conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations, which raise questions concerning the Individual's reliability, trustworthiness and ability to protect classified information. Adjudicative Guideline E at ¶ 15.

Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information. Adjudicative Guideline M at ¶ 39. Guideline M further provides that "introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations" are among those "Conditions that could raise a security concern and may be disqualifying." Adjudicative Guideline M at ¶ 40(f).

---

[4] At the Hearing the Individual testified: "Having hindsight now and seeing how it can be perceived and the perception, I would do things differently of course. And especially with my knowledge of how the DOE looks at these kind of things and how it can be perceived as almost criminal. I mean, I was charged criminally for this stuff. I definitely would do it differently." Tr. at 139.

[5] Under the circumstances of the present case, I find that the alleged security concerns arising from the Individual's three extra-marital affairs do not raise significant security concerns. The Individual has testified that these affairs occurred during a period in which he and his wife had planned to divorce and he thought that his marriage was ending. Tr. at 175-176. Moreover, his wife is now aware of these three affairs, he is therefore not at risk for extortion or coercion as a result of these affairs. Tr. at 148-149.

## V. ANALYSIS

The Individual, attempting to establish mitigation of the security concerns raised by derogatory information discussed above, has raised a number of arguments. After careful consideration of each of these arguments and the record, I find that the Individual has not sufficiently mitigated the security concerns raised under Guidelines E or M, or Criterion L.

First, the Individual argues that he copied the information at issue because he was afraid that Owner A would accuse him of deleting files. I am convinced that the Individual's motivation for copying the contents of Employer A's laptop's hard drive onto his external hard drive was self-protection. There is no evidence in the record showing that the Individual intended to provide Employer B with the information he uploaded into his external hard drive. Nor is there any evidence in the record that Employer B accessed or otherwise used the information in the external hard drive. While both factors provide some mitigation of the severity of the security concerns raised by the Individual's actions, the Individual's decision to copy the contents of the laptop onto his personal external hard drive nevertheless demonstrated a serious deficiency of judgment, reliability, and loyalty.

Second, the Individual argues that there is no evidence in the record that Employer B has accessed or used any of the information stored on the hard drive. Regardless, the Individual should not have misappropriated the information stored on the hard drive.

Third, the Individual argues that the State Court found that the non-disclosure agreement that the Individual signed was unenforceable. However, the fact that the non-disclosure agreement was not enforceable under law does not fully mitigate the security concerns raised by the Individual's decision to violate a written commitment that he made to his employer. *See* Adjudicative Guidelines ¶ 16(f).

Fourth, the Individual now claims that none of the information on the hard drive was confidential or proprietary. This claim is contradicted by the findings of the State Court, as well as the Individual's own description of the contents of the external hard drive, as discussed above in the Findings of Fact section.

Fifth, the Individual notes that the State Court jury verdict is under appeal, and contends that this Appeal is likely to succeed because "there are serious questions about whether [Employer A] can sustain its damage theory on appeal." Tr. at 308. I am unwilling and unable to speculate about the eventual outcome of this appeal.

Sixth, the Individual notes that a number of people have testified to his good character and honesty. While this testimony is a positive factor, it alone cannot mitigate the security concerns discussed at length above.

Seventh, I find that the Individual's claims that he had no intent to harm Employer A are not fully credible in light of the Individual's comments concerning Owner A. During his PSIs and his testimony at the Hearing, he made a number of strong allegations about Owner A (including accusing Owner A of blackmailing two former owners and insinuating that Owner A was under

investigation by the Federal Bureau of Investigation). Tr. at 121-125. More importantly, even if I were to find the Individual's contention that he did not intend to harm Employer A credible, it would not provide any mitigation of the security concerns at issue.

Finally, the Individual correctly notes that five years have passed since the behaviors which raised the security concerns at issue occurred. He claims that he is now a better, changed person. I am not convinced. During the present proceeding, the Individual has consistently failed to acknowledge the magnitude of his lapses in judgment or express regret for his actions, other than to admit that they have caused him inconvenience. For example, when the Individual was first asked by the LSO to discuss and explain the civil law suit, he assured the interviewer that the suit was frivolous. As recently as the March 14, 2012, PSI, he described his decision to download the contents of Employer A's laptop computer to his external hard drive as "very wise." DOE Exhibit 2 at 14. Throughout this proceeding, he attempted to shift the blame for his actions onto Owner A, without recognizing that any of his own actions were highly improper.

As for his provision of confidential or proprietary information concerning employee salaries and qualifications to Employer B, in the August 20, 2007, email, the Individual asserts: (1) the information he provided was not proprietary or confidential, and (2) he was not attempting to provide information about specific individuals in order to allow them to be hired away from Employer A by Employer B, but rather was estimating the expected costs for Employer B to expand its Quality Assurance program by adding additional employees with specific qualifications. However, the Individual's civil trial testimony and the plain language of the email itself both contradict these assertions.

Based on all the foregoing, I find that the security concerns under Criterion L raised by the Individual's personal conduct remain unresolved.

## V. CONCLUSION

For the reasons set forth above, after carefully considering the evidence before me, I find that the Individual has not resolved the security concerns raised under Criterion L. Therefore, the Individual has not demonstrated that restoring his security clearance would not endanger the common defense and would be clearly consistent with the national interest. Accordingly, I find that the Individual's security clearance should not be restored. The Individual may seek review of this Decision by an Appeal Panel under the procedures set forth at 10 C.F.R. Part 710.28.

Steven L. Fine
Hearing Officer
Office of Hearings and Appeals

Date: October 22, 2012