* 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:	May 16, 2012	)	
		)	Case No.: PSH-12-0060
		)	

Issued: September 14, 2012

Hearing Officer Decision

William M. Schwartz, Hearing Officer:

This Decision considers the eligibility of XXXXXXXXXXX (the individual) to hold an access authorization[1] under the regulations at 10 C.F.R. Part 710, entitled "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material." As I explain below, the Department of Energy (DOE) should restore the individual's access authorization.

I. Background

The individual is employed by a DOE contractor and has held a DOE access authorization since 2009. During a routine polygraph examination, the individual revealed that he had failed to comply with rules and procedures regarding information technology systems. These admissions prompted the Local Security Office (LSO) to conduct a Personnel Security Interview (PSI) with the individual in January 2012. Ex. 10.

Because the PSI did not resolve the security concerns raised by the individual's admissions, the LSO issued the individual a Notification Letter in May 2012, advising him that it possessed reliable information that created a substantial doubt about his eligibility to hold an access authorization. Ex. 1. In an attachment, the LSO explained

[1] An access authorization, also known as a security clearance, is an administrative determination that an individual is eligible for access to classified matter or special nuclear material. 10 C.F.R. § 710.5.

that the derogatory information falls within the potentially disqualifying criterion in the security regulations at 10 C.F.R. § 710.8(l) (Criterion L).[2]

After the individual received the Notification Letter, he invoked his right to an administrative review hearing. Ex. 2. On May 17, 2012, the Director of the Office of Hearings and Appeals (OHA) appointed me Hearing Officer, and I conducted the hearing. The DOE counsel introduced 11 numbered exhibits into the record, and the individual tendered 12 exhibits (Exhibits A through L). The individual testified on his own behalf and called as witnesses four co-workers and a psychiatrist.

II. Regulatory Standard

The regulations governing the individual's eligibility for access authorization are set forth at 10 C.F.R. Part 710, "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material." The regulations identify certain types of derogatory information that may raise a question concerning an individual's access authorization eligibility. 10 C.F.R. § 710.10(a). Once a security concern is raised, the individual has the burden of bringing forward sufficient evidence to resolve the concern.

In determining whether an individual has resolved a security concern, the Hearing Officer considers relevant factors, including the nature of the conduct at issue, the frequency or recency of the conduct, the absence or presence of reformation or rehabilitation, and the impact of the foregoing on the relevant security concerns. 10 C.F.R. § 710.7(c). In considering these factors, the Hearing Officer also consults adjudicative guidelines that set forth a more comprehensive listing of relevant factors. *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).

Ultimately, the decision concerning eligibility is a comprehensive, common-sense judgment based on a consideration of all relevant information, favorable and unfavorable. 10 C.F.R. § 710.7(a). In order to reach a favorable decision, the Hearing Officer must find that "the grant or restoration of access authorization to the individual would not endanger the common defense and security and would be clearly consistent with the national interest." 10 C.F.R. § 710.27(a). "Any doubt as to an individual's access authorization eligibility shall be resolved in favor of the national security." *Id*. *See generally Dep't of the Navy v. Egan*, 484 U.S. 518, 531 (1988) (the "clearly consistent with the interests of national security" test indicates that "security clearance determinations should err, if they must, on the side of denials").

[2] Criterion L includes "unusual conduct" and "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." *Id*. at § 710.8(l).

III. The Notification Letter and the Security Concerns

The LSO supported its Criterion L security concern with the following allegations:

- In the summer of 2009, the individual watched a pornographic DVD on his government computer; he had also viewed pornography on a government computer in 2007 and earlier in 2009 while working for a different employer, knowing that this activity was against policy;

- In 2009, the individual used a personal thumb drive to copy a file from his government computer to his personal computer;

- In November 2011, the individual took pictures with his personal camera and then downloaded them to his government computer;

- In a January 2012 PSI, the individual admitted that each of the above incidents had occurred, that he had not reported them to security at the time they occurred, and that he had committed, and reported, three security incidents between 1988 and the late 1990s; nevertheless, he had failed to acknowledge any of these incidents in an earlier PSI conducted in May 2011; and

- Despite the 2009 thumb drive incident, the individual certified on a September 24, 2010, Questionnaire for National Security Positions (QNSP), that in the preceding seven years, he had not introduced media into an information technology system in an unauthorized manner.

Ex. 1.

I find that the above information constitutes derogatory information that raises questions about the individual's conduct under Criterion 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. Adjudicative Guidelines at Guideline E, ¶ 17. Further, 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. *Id.* at Guideline M, ¶ 39.

IV. Findings of Fact

The individual has held a security clearance since 1988. Transcript of Hearing (Tr.) at 175. In 2007, while working for a different federal agency, he viewed pornographic websites from his government computer, and his supervisor counseled him verbally, telling him to "knock it off." *Id.* In late 2008 or early 2009, he viewed pornographic videos on the Google Video website. *Id.* His employer suspended some of his classified access privileges for a year as a result of his misuse of computer resources. Ex.10

(Transcript of Personnel Security Interview, January 12, 2012) at 53. He recognized that he was addicted to pornography, *id*. at 60, and voluntarily sought help. Tr. at 176. He was evaluated by a psychiatrist who testified at the hearing that the individual did not suffer from a diagnosable mental condition. *Id*. at 21. He stated that the individual did have a longstanding "compulsive or addictive need to view pornography," and recommended treatment with a psychologist. *Id*. at 21, 25.

The individual met weekly with the psychologist for a year, and attended Sex Addicts Anonymous (SAA) meetings concurrently with the treatment and continued attending for an additional six months beyond the period of treatment. *Id*. at 177. In the summer of 2009, shortly after he assumed his current position, and early in his treatment with the psychologist, the individual purchased a pornographic magazine that contained a DVD and inserted the DVD into his government laptop computer. *Id*. at 183-84. After a few minutes, he realized that he "was being incredibly stupid," removed the DVD and threw it away. *Id*. at 184. He admitted this lapse to his SAA sponsor, and possibly to his therapist, but he did not inform his employer. *Id*. at 185. He continued with his therapy and SAA meetings and has had no additional problems involving pornography. *Id*. at 180, 185. At the hearing, the individual's psychiatrist expressed his opinion that the individual is very unlikely to view pornography in the future. *Id*. at 26.

Also shortly after assuming his current position in 2009, the individual needed to print a file stored on his government computer. Due to unusual circumstances, the only available printer was attached to his personal computer. He used a personal thumb drive to copy a file from his government computer, inserted the thumb drive into his personal computer and printed the document. *Id*. at 192. In September 2010, the individual completed a Questionnaire for National Security Positions (QNSP), in which he certified that he had not "introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations." Ex. 8 at Section 27(c).

During a May 2011 PSI, the individual stated that he had not viewed pornography since February 2009, despite the DVD episode described above. Ex. 11 (Transcript of Personnel Security Interview, May 5, 2011) at 76-78. During the same PSI, he did not include the above-described thumb drive episode when asked to enumerate past security violations. *Id*. at 134.

In November 2011, the individual used his personal camera to take photographs related to a work project. He then copied the pictures to his government computer to include them in a report he was preparing. Tr. at 186. At the time, he was not aware that he had violated any security policy. He explained at the hearing that in past situations he had hired a photographer to perform this function, but the project had spent all its funding. He had no funding to hire a photographer, and so he had to take the pictures himself. *Id*. at 188. Although he reported the incident to his co-worker, who admonished him not to repeat it, he did not report it to the LSO. *Id*. at 191.

In late November 2011, the individual was subjected to a polygraph examination. *Id*. at 189; Ex. 8. Explaining the meaning of the questions that would be asked during the examination before the actual testing began, the polygraph examiner produced a document that illustrated numerous security violations. When the individual studied the document, he realized that he had committed two violations: when he used the thumb drive to transfer a file, and when he copied photographs from his personal camera to his government computer. Tr. at 190.

The LSO conducted a second PSI with the individual in January 2012. At that PSI, the individual provided a number of facts of which the LSO had not been aware. He admitted that he had viewed a pornographic DVD on his government laptop in the summer of 2009. In addition, he admitted to the 2009 thumb drive and 2011 camera incidents. Ex. 10. Finally, he disclosed three events that took place between 1988 and the late 1990s in which he may have mishandled classified material. He had reported all of these incidents when they occurred, but had not recalled them during his May 2011 PSI. Tr. at 198-203. At the hearing, he testified that his experience at the polygraph examination had caused him to recall all of these incidents. *Id*. at 200.

V. Analysis

A. Testimony at the Hearing

At the hearing, a number of witnesses offered their opinions concerning the individual's general adherence to security policy and the incidents that raised LSO's concerns. The individual's psychiatrist noted that the individual had received appropriate treatment for his pornography compulsion. He testified that the individual's 2009 momentary lapse in judgment, when he introduced the DVD into his government computer, occurred early in his treatment and is not at all an uncommon occurrence. *Id*. at 27, 29-30, 38-39. He also expressed his opinion that the individual had not willfully or intentionally disregarded security policy when he used his thumb drive and personal camera improperly; in both cases, he did not have security protocols on his mind but rather was focused on getting the necessary work accomplished. *Id*. at 27, 36.

Four additional witnesses testified on behalf of the individual. Each has worked with him closely for at least 13, and as long as 24, years. Each testified that the individual has a reputation for following rules and regulations and treating classified material with care. *Id*. at 67, 88-89, 115, 140-41, 146, 154. They were aware of his difficulties with pornography because he had discussed the problem with them. They were also aware that he received treatment for this problem and had no concerns that this would raise any work-related issues in the future. *Id*. at 68, 90, 143. They uniformly stated that the thumb drive and camera incidents were not intentional breaches of security policy but rather decisions the individual made in order to serve the needs of his program. *Id*. at 70, 75, 93-94, 120-22, 151, 154. Two of the witnesses specifically spoke to the individual's truthful nature, and a third pointed out that a recent scan of the individual's computer revealed no recent improper use of any sort, and that the individual is firmly committed to not repeating any of the mistakes he has made. *Id*. at 94, 123, 152, 156.

The individual's testimony focused on explaining why he violated security practices, why he did not report the violations, and why he will not repeat such incidents in the future. After having his clearance suspended in 2009 for viewing pornography at work, the individual immediately sought treatment. *Id*. at 176. He understood his then-employer's concerns regarding both his personal conduct and his misuse of computer resources. *Id*. He had one relapse to viewing pornography shortly after he began his treatment, and realized within a few minutes of inserting the DVD into his government laptop that he was violating his employer's policy. *Id*. at 184. He has fully controlled his addiction since completing his therapy nearly three years ago. *Id*. at 185. He maintains that the DVD incident, in the summer of 2009, is the last time he has intentionally violated a security policy. *Id*. at 225.

The individual testified that his two most recent security violations—the 2009 thumb drive incident and the 2011 camera incident—were unintentional. At the time he used his personal thumb drive to copy a file from his government computer, he did not think that he had violated any security rule or policy in this manner, and did not inform his employer or the LSO. *Id*. at 193. Nor did that possibility occur to him while he was completing a QNSP in September 2010, when he responded in the negative to a question that specifically asked whether he had "introduced . . . or media in connection with any information technology system without authorization." *Id*. at 204. He testified that he did not recall the incident when completing his QNSP, and recalled it for the first time only during the polygraph process in November 2011. *Id*. Similarly, he testified that he did not realize at the time that it was improper to copy photographs from his personal camera to his government computer. He stated that, in light of his profession and education, "You'd think I'd know better, but I didn't think camera, data storage device. I just didn't make the connection." *Id*. at 187. As with the thumb drive incident, the individual realized that this activity violated employer policy only during the polygraph process. *Id*. at 188-90. He further testified as to how he would handle the same situations if they were to occur again, without breaching security policy. *Id*. at 191, 193. Finally, he addressed the steps he has taken since the polygraph examination to improve his security practices, including keeping a copy of the security rules on his office desk, calling security officers in two locations, never using his personal thumb drive or camera again for government work, and repeating a cyber-security refresher course. *Id*. at 204-07.

The individual also addressed the discrepancies between his May 2011 PSI, at which he failed to disclose the 2009 DVD and thumb drive incidents, and his disclosure of them at the January 2012 PSI, which took place after the polygraph examination. As discussed above, it was not until the polygraph examination that he realized that either of those incidents concerned potential breaches of security. *Id*. at 188-90, 193. For that reason as well, he did not report either event to the LSO. *Id*. at 186, 193. He also failed to recall three security incidents that occurred early in his career, between 1988 and the early 1990s, which he had reported at the time. He stated that he never tried to hide the incidents and had no fear of reporting, but that the polygraph procedure made him realize and recall his errors in a way that nothing else had to that point. *Id*. at 229-30. To avoid the possibility of future inconsistent statements in the future, the individual has created a

document in which he has recorded all of his past security breaches, so that he need not rely on his memory to fully disclose to the LSO should the need arise in the future. *Id*. at 206.

B. Hearing Officer's Opinion

To determine whether the individual has mitigated the allegations and therefore resolved the security concern, I will consider the relevant factors from 10 C.F.R. § 710.7(c) and the relevant mitigating conditions from the Adjudicative Guidelines, Guideline E (Personal Conduct) and Guideline M (Use of Information Technology Systems).[3]

I assign positive weight to several factors. The individual presented evidence suggesting that he has a low likelihood of continuing his misconduct. His witnesses uniformly praised the care with which he treats sensitive information. The psychiatrist's prognosis

[3] Guideline E contains the following relevant mitigating conditions:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before confronted with the facts;
>
> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and
>
> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused the untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

Adjudicative Guidelines at Guideline E, ¶ 17.

Guideline M contains the following mitigating conditions:

> (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
>
> (b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness . . .; and
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

Id. at Guideline M, ¶ 41

There is no requirement that any particular number of factors or conditions be proved or that a majority of them point one way or the other. The relevance of each factor and condition depends on the facts. In this case, certain factors and conditions may demonstrate mitigation, but in other cases, other factors and conditions may do so. Adjudicatory review is not a mechanical point-counting device. Rather, the Hearing Officer looks at the totality of the circumstances to make a common-sense, reasoned judgment whether the individual has mitigated the allegations to resolve the security concern or concerns raised by the agency.

of the individual's involvement with pornography was very favorable, and there is no evidence that the individual has viewed pornography in three years. He has had a successful career with an access authorization, and since the November 2011 polygraph examination, at which he asserts he realized his errors, he has not engaged in any questionable security practices. Finally, though the individual has provided inconsistent information regarding his past security incidents, I note that his more recent statements made during the January 2012 PSI—following the polygraph examination—represent a fuller, and more honest, disclosure than his earlier statements.

Nevertheless, I must also consider a number of negative factors that these circumstances present. The individual took no corrective action concerning his pornography compulsion or addiction until his employer confronted him. With respect to the thumb drive and camera incidents, he made no efforts to correct his failure to report them to his employer or to the LSO during a PSI until after the polygraph examination. Although the individual maintains that he was unaware of his errors before the polygraph and therefore did not realize he had anything to report, a polygraph examination, and the pressure to pass one, are hardly circumstances that demonstrate the individual's good faith and free will in voluntarily disclosing security violations.

The overarching concern is whether the individual will act in the future in a manner that places the national security at risk. The record of this case convinces me that it is highly unlikely that the individual will ever again view pornography on a government computer, or introduce a personal thumb drive or personal camera connection into a government computer. As discussed above, the individual's completion of a treatment program that addressed his pornography compulsion or addiction, and the passage of three years since that treatment, during which time the individual has had no events involving pornography, strongly demonstrates that the likelihood of a relapse is extremely low. During those three years, however, the individual committed two unintentional, isolated, and relatively minor security errors. He explained at the hearing that both occurred under unusual circumstances that are unlikely to recur. He used his personal thumb drive because his government-issued thumb drive had been recalled and he had not yet been issued its replacement. Moreover, the printer that had been connected to his government computer had broken, and its replacement had not yet been configured for operation. Tr. at 192. He used his personal camera because his project budget did not contain enough money to hire a professional photographer, as he had done in the past, to take pictures of the project's results to include in a required report. *Id*. at 187-88. In both instances, his job required that he provide the information he collected on those media to others in quick order. The individual's testimony clearly shows that he fully understands that these actions were improper and demonstrates how he will handle such situations in the future, should they arise, in an appropriate manner, including reporting any information technology errors that are contrary to employer policy. To his credit, he recently reported an improper computer-printer connection in his office. *Id*. at 209-11.

One remaining concern is that the individual professed ignorance of the policies he violated when he used the thumb drive and camera as described above. The individual himself testified that he should have realized that it was improper to connect his camera

to his government computer. While he acknowledged that using his thumb drive as he did was unusual, he testified that he "wasn't really thinking about it." *Id*. at 193. I recognize that in both instances, the individual was under time constraints and took those actions in the interest of organizational efficiency and effectiveness. On the other hand, any holder of a security clearance must be held responsible for knowing how to use technology systems correctly and without endangering the DOE's national security. The individual explained the steps he has recently undertaken to improve his compliance with security policies, including repeating a cyber-security refresher course. These steps have raised the individual's awareness of security concerns and are to be praised. I believe that these corrective steps, together with the humbling experience of this administrative review process, have raised the individual's awareness such that he will be appropriately vigilant in the future. Consequently, I find that the individual has mitigated the LSO's concerns regarding his unauthorized use of government technology systems, his noncompliance with rules pertaining to such systems, and his honesty, reliability and trustworthiness.

VI. Conclusion

Because the individual has resolved the Criterion L security concern, I find that he has demonstrated that restoring his access authorization would not endanger the common defense and would be clearly consistent with the national interest. Therefore, I find that the DOE should restore his access authorization.

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

William M. Schwartz
Hearing Officer
Office of Hearings and Appeals

Date: September 14, 2012