

* 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 XXXXXXX's.

February 18, 2004
DEPARTMENT OF ENERGY

OFFICE OF HEARINGS AND APPEALS

Hearing Officer's Decision

Name of Case: Personnel Security Hearing
Date of Filing: June 2, 2003
Case Number: TSO-0058

This Decision concerns the eligibility of XXXXXXXXXX (hereinafter referred to as the "individual") to hold an access authorization 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." A Department of Energy Operations Office (DOE Operations Office) suspended the individual's access authorization under the provisions of Part 710. This Decision considers whether, on the basis of the evidence and testimony presented in this proceeding, the individual's access authorization should be restored. As set forth below, it is my decision that the individual's security clearance should not be restored.

I. Background

The individual is employed at a DOE facility, and held an access authorization as a requirement of his job. In August 2002, an audit of the computers at the individual's workplace disclosed that the individual had accessed Websites containing sexually explicit material. In October 2002, DOE conducted a Personnel Security Interview (PSI) with the individual. The DOE suspended the individual's access authorization in November 2002 as a result of derogatory information that is set forth in the Notification Letter, and is summarized below.

The Notification Letter states that the derogatory information regarding the individual falls within 10 C.F.R. § 710.8(g) and (l) (Criteria G and L). The DOE Operations Office invokes Criterion G on the basis of information that the individual has failed to protect classified matter, or safeguard special nuclear material; or violated or disregarded security or safeguards regulations to a degree which would be inconsistent with the national security; or disclosed classified information to a person unauthorized to receive such information. In this regard, the Notification Letter states that: (1) the individual regularly accessed adult entertainment sites using a DOE computer despite signing user agreements that clearly state that government resources are for government business only; (2) the individual downloaded unauthorized programs from

the Internet, may have attempted to participate in chat rooms, and may have had unapproved installation of an Internet chat application ; and (3) forensic analysis of files on the individual's computer detected seven "cookies" related to sexually explicit adult Websites. ¹ The DOE Operations Office invoked Criterion L on the basis of information that the individual engaged in unusual conduct or is subject to circumstances which tend to show that he is not honest, reliable, or trustworthy; or which furnishes reason to believe that he may be subject to pressure, coercion, exploitation or duress which may cause him to act contrary to the best interests of the national security. In regards to Criterion L, the Notification Letter stated that: (1) the individual had deliberately accessed sexually explicit adult material (SEAM) and may have accessed an Internet Relay Chat program with "phone home" features; (2) multiple proxy logs for the individual's user ID corresponded to the date and time stamps of images found on the individual's system; and (3) the individual intentionally downloaded SEAM and accessed unauthorized sites until his activity was discovered by DOE in the summer of 2002. ²

In a letter to DOE Personnel Security, the individual exercised his right under Part 710 to request a hearing in this matter. 10 C.F.R. § 710.21(b). On June 4, 2003, I was appointed as Hearing Officer in this case. After conferring with the individual and the appointed DOE counsel, 10 C.F.R. § 710.24, I set a hearing date. At the hearing, the DOE counsel called two witnesses, a DOE personnel security specialist and a DOE Information Systems manager. The individual testified and also elected to call three colleagues, an Internet crime expert, and his wife as witnesses. The transcript taken at the hearing shall be hereinafter cited as "Tr." Various documents that were submitted by the DOE counsel during this proceeding constitute exhibits to the hearing transcript and shall be cited as "Ex." Documents that were submitted by the individual during this proceeding are also exhibits to the hearing transcript and shall be cited as "Indiv. Ex."

After the hearing, the record was held open for the receipt of computer logs which had been referenced, but not entered into evidence at the hearing. Those logs were sent to all parties in September 2003. The individual's attorney then requested the opportunity to take telephone testimony regarding the preparation and interpretation of the logs. The parties took additional testimony in November 2003, and the record was closed upon receipt of the transcript of the supplemental testimony in December 2003. That transcript shall be cited as "Tr. II."

1/ A "cookie" is a small file that a Web server automatically sends to a user's personal computer when the user browses certain Web sites. Cookies contain identifying information about the user that eliminates the need for the user to reenter the information on subsequent visits.

2/ Prior to the hearing, the DOE IS group determined that the individual did not access an Internet Relay Chat program with "phone home" features. Tr. at 113-115; Ex. 15.

II. Analysis

The applicable 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 of access authorization would not endanger the common defense and security and would be clearly consistent with the national interest.” 10 C.F.R. § 710.7(a). Although it is impossible to predict with absolute certainty an individual’s future behavior, as the Hearing Officer, I am directed to make a predictive assessment. There is a strong presumption against the granting or restoring of a security clearance. *See Department of Navy v. Egan*, 484 U.S. 518, 531 (1988) (“clearly consistent with the national interest” standard for the granting of 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).

I have thoroughly considered the record of this proceeding, including the submissions of the parties, the evidence presented and the testimony of the witnesses at the hearing convened in this matter. 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): 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 of the individual at the time of the conduct; the voluntariness of the 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 continuance or recurrence; and other relevant and material factors. After due deliberation, it is my opinion that the individual’s access authorization should not be restored as I cannot conclude that such restoration would not endanger the common defense and security and would be clearly consistent with the national interest. 10 C.F.R. § 710.27(a). The specific findings that I make in support of this determination are discussed below.

A. Findings of Fact

The individual has been employed by the DOE for a number of years in a job that required that he maintain a security clearance. Ex. 13 at 5. The individual received his clearance in 1986. Ex. 6. at 1. His job required frequent travel. Tr. at 172, 176. Because the individual and his colleagues spent most of their duty time on the road, the managers of his local office purchased desktop computers that could be accessed by multiple users in order to avoid the unnecessary expense of buying one computer for each employee. Tr. at 177. In 1998, the individual first received a user identification (“user ID”) number and password for unclassified systems in order to check his electronic mail. Ex. 16. The individual and his colleagues did not receive specific training on the computer. Tr. at 180, 211. In 2002, the individual and his colleagues were given access to the Internet. Ex. 21 at 3; Ex. 15 at 2. According to the individual, when he was in the home office between assignments, he searched Google using the keywords “guns, firearms, fitness.” PSI (Ex. 12) at 7. The individual did this because he was bored and could not think of

anything more creative to do with his “downtime.” PSI at 13. When he was bored, he would surf the Internet for a couple of hours in the morning and a couple of hours in the afternoon. PSI at 11-13. The Google search produced 80 to 90 pages of “hits,” and the individual would spend his time accessing every website that was listed under the search results. PSI at 10. Some of the sites contained sexually explicit material. PSI at 8-12. The individual stated that he intentionally downloaded the pictures, and attributed his actions to “poor judgment,” explaining that he could not think of anything more creative to do during the time that he was in the office and not assigned to a specific task. PSI at 13. He also admitted to “wasting time with other things,” like crossword puzzles. PSI at 14. In June 2002, the individual signed a form acknowledging that he understood the Code of Conduct for general users of his facility’s information systems, including “protecting against waste, fraud, and abuse involving information systems.” Ex. 18.

In August 2002, a management official in the individual’s local office ordered all computers to be physically audited for waste, fraud, and abuse. Tr. at 36; Ex. 23. The computers were audited on August 22-23, 2002. Ex. 23. A local systems administrator found SEAM on an office computer under the individual’s user ID, and the information systems (IS) manager then ordered the machine impounded in order to perform a full audit of the machine. Tr. at 37-38. After the audit, the IS group found approximately 35,000 graphic images on the computer, of which approximately 140 were SEAM. Tr. at 38, 49; Ex. 15. The IS manager concluded that the individual had surfed adult entertainment sites from April to August 2002 on a regular basis. Tr. at 40. Local management immediately barred the individual from accessing the Internet. Tr. at 187-192. In September 2002, the individual was removed from the Personnel Assurance Program (PAP) by the PAP administrator and a senior manager. Tr. at 192; Ex. 23. The individual was counseled about his use of the computer and given tasks that he could complete without access to Internet or electronic mail. *Id.* at 194. Local management disciplined the individual with three days suspension without pay and a six month suspension of his Internet access. Tr. at 194-196.

A site clinical psychologist evaluated the individual on October 1, 2002. PSI at 23; Ex. 21. In addition to an interview, the psychologist also contacted the individual’s supervisor and reviewed the individual’s yearly psychological evaluations since 1994. Ex. 21. The psychologist concluded that the individual’s unauthorized use of the computer did not stem from an impulse control problem or personality style that would predispose the individual to those actions. Ex. 21 at 3. There was no evidence of an antisocial personality disorder, and nothing to suggest that the individual’s actions were more than random acts resulting from boredom or curiosity. *Id.* During the interview, the individual expressed surprise that he got in trouble for his unauthorized computer use. *Id.* The psychologist then recommended that the individual participate in additional one-on-one training in computer security “in light of the attitude that he [the individual] did not feel like he had done anything wrong.” *Id.*

DOE security considered the individual’s accessing of sexually explicit material on a government computer to be “waste, fraud, and abuse” under the terms of the audit. Tr. at 34. As a result of the audit, DOE security conducted a PSI with the individual on October 8, 2002 in order to resolve the derogatory information. Ex. 12. After the PSI, the personnel security specialist recommended no further action because the individual had received a favorable psychological evaluation and the violation “appeared to

be an isolated incident.” Ex. 2; Tr. at 26. The specialist’s supervisor disagreed with that conclusion and found that the unauthorized use was not only deliberate, but had also occurred over a long period of time. Ex. 2. The supervisor recommended that the case proceed through the administrative review process. *Id.*

The individual’s clearance was suspended on November 19, 2002. Letter from Individual to DOE (May 1, 2003). On March 31, 2003, the individual was suspended indefinitely without pay pending the final resolution of his eligibility for access authorization. Indiv. Ex. 4. On May 1, 2003, the individual requested a hearing. *Id.*

B. DOE’s Security Concern

According to local DOE security personnel, the individual’s unauthorized use of a DOE computer to access sexually explicit material created a concern regarding the individual’s judgment and reliability –specifically, why the individual would do this at work given knowledge of the rules and regulations regarding such activity. Tr. at 24. He had signed user agreements that clearly state that government resources are for government business only. Tr. at 24; Ex. 1 at 1; Ex 16; Ex. 18. The individual had also received two electronic mail messages, in May 2000 and August 2002, from senior management with the following information on appropriate use of the Internet during work hours:

Unauthorized uses of Internet and email technology include, but are not limited to, those that: (1) result in a loss of productivity; (2) impair the performance of the network; (3) are unlawful or offensive to fellow employees or the public (e.g., gambling, hate speech or material that ridicules on the basis of race, creed, religion, color, sex, national origin, disability, or sexual orientation); (4) transmit sexually explicit or sexually oriented material; or (5) allow unauthorized access to controlled information (e.g., computer software, privacy information, classified or other non-public data, copyright, trademark or other intellectual property rights).

Ex. 17, 19 One of those messages was distributed to persons at the individual’s site in August 2002, after DOE alleges that the individual had been accessing unauthorized sites for four months. In addition, the forensic analysis of the individual’s computer detected seven “cookies” related to SEAM websites in the individual’s user ID. According to the DOE IS manager, SEAM websites present a security risk because they often transmit malicious code, information about the user’s computer, and may scan a computer for exploitable vulnerabilities. Ex. 14. In addition, a reasonable person would realize that SEAM is prohibited at a workplace. *Id.* Finally, local DOE security was concerned because the individual continued his unauthorized use of the computer over a long period of time, and did not stop until he was discovered by the audit in August 2002. Surfing the Internet and accessing this type of material at work raises questions about the individual’s judgment and whether he may ignore regulations and decide which rules he wants to follow. See Tr. at 24; PSI at 26. See also *Personnel Security Review*, OHA Case No. VSO-0435, 28 DOE ¶ 82,804 (2001), *affirmed* (OSA, October 2, 2001) (pattern of disregard for government

computer policy raises concerns about individual's honesty, reliability, and trustworthiness). Based on the above, I find that DOE correctly invoked Criteria G and L.

C. Hearing Testimony

1. The Individual

The individual testified at the hearing that he had unintentionally accessed sexually explicit websites because he was not familiar with the use of computers and the Internet. Tr. at 74, 82-83. He also maintained that he had never seen most of the sexually explicit pictures that the IS group claimed to have discovered under his user ID. *Id.* at 81. The individual further alleged that he admitted to intentionally downloading the pictures during his PSI only because he wanted to accept responsibility for his actions and did not want to argue with the personnel security specialist. *Id.* at 90-92. He also assumed that his activities were monitored constantly by his headquarters IS group and that he would be notified immediately if he did something wrong or accessed inappropriate material. *Id.* at 76.

The individual testified that while surfing the Internet in his downtime at the office, his searches on fitness and firearms produced hundreds of listings of websites, some with sexually explicit content. *Id.* at 74. He admitted that he was aware of the DOE's prohibition on the transmission of SEAM. Tr. at 74. The individual said that when he entered a work-related topic (e.g. guns, firearms, muscle, fitness), the ensuing Google search would return with 80 or 90 pages of topics. *Id.* at 75. He would try to think of a way to get through all of the pages, sometimes beginning with the first page and sometimes beginning with the last page. *Id.* The individual maintained that he did not intentionally search for, download, or save any SEAM. *Id.* at 81. The individual also testified that he did not see most of the pictures that DOE alleges were found on his computer. Tr. at 94.

2. The DOE Information Systems Manager

The DOE Information Systems (IS) manager responsible for computer security at the site testified that he began working in his present capacity in January 2002. Tr. at 35. At that time, site policy prohibited all personal use of the Internet. *Id.* at 66. The manager explained how his office would typically detect the unauthorized use of government computers. A server logs an individual's user ID and also logs every website that the individual accesses through that server. *Id.* at 44. The server has filters that drop log entries into specific files based on categories. *Id.* For example, well-known adult website names are put into the "smut log," and if an individual accesses one of those sites, an entry is made in the log. *Id.* If there is a pattern of accesses, the IS group investigates, and if there is a pattern of continual or long term abuse, the IS will physically confiscate the computer. *Id.* If a user exhibits occasional unauthorized use, the IS group will send the user a warning email. *Id.* at 43. The IS group then examines the machine for any additional evidence, such as pictures being downloaded, and issues a report to management. *Id.* at 44-45.

However, the IS group did not detect the individual's usage in that manner. The individual's behavior was not spotted in the firewall logs because the normal daily review of the logs did not begin until June 2002. *Id.* at 65. ³ The IS manager testified that in August 2002, after the local system administrator found unauthorized material under the individual's identification number, the IS staff performed a forensic analysis of his machine. *Id.* at 37-38. Based on his interpretation of the audit results, the manager concluded that the individual had surfed various adult entertainment sites, and that some of the files were still on his computer. Tr. at 40. The manager concluded that the accesses were not inadvertent because the individual accessed the sites on a regular basis over a period of four months. *Id.* The individual's unauthorized use was "regular, but it was not extensive." *Id.* at 47.

At the hearing, the IS manager explained how he determined that the individual had accessed some of the websites intentionally. The IS group found approximately 35,000 graphic images on the individual's computer, of which approximately 141 were sexually explicit. *Id.* at 49. The dates of the sexually explicit graphics matched dates in the individual's user ID account and the cookies matched with the firewall logs. *Id.* at 53. The IS group could find a cookie for a certain date under the individual's user profile, go back to the firewall logs and find that his user ID had visited that website, and thus find a correlation between the firewall log and the individual's local profile. *Id.* at 53.

The IS manager testified that "there is really no way to know how long the person has been on [a particular website] because the individual computer and the firewall proxy only log when somebody goes out and gets additional content." Tr. at 104. The log file tells when a user clicks for more content, "it will not tell you how long a person sat there looking at a picture." Tr. at 111-112. The IS group concluded that the individual's use was "occasional but intentional." *Id.* at 113. Even though the individual was not spending hours on the computer, the IS group saw indications that he intended to visit certain unauthorized sites. *Id.* The manager testified that a user's return to certain sites over a period of time indicates to him that the activity is probably intentional. *Id.* at 98. Based on repeat activity, the manager found that some of the individual's accesses were intentional. *Id.* According to the manager, if a user backs out of a site immediately, some images will not be downloaded. Tr. at 100. He admitted that a user can easily end up on a website unintentionally, but some of the sites that the individual accessed repeatedly had names that were obviously sexually explicit (e.g., "sextracker.com"). *Id.* at 102, 105.

The manager explained that neither the individual or his supervisor questioned the report at the time it was issued. *Id.* at 55. He testified that the IS group provides "as much detail as we feel that the management needs to take some action. If somebody comes back and says, I didn't do that, or that was not my user ID . . . then we go back and we look further at it." *Id.* at 55. Based on previous experience with

^{3/} The DOE IS manager was hired in January 2002. The IS staff normally checked logs daily for suspicious unauthorized activity. Tr. at 65. However, this daily check ceased in June 2001 when the position of IS manager became vacant, and did not resume until June 2002. Tr. at 45, 65. Now, if a user exhibits occasional unauthorized use, the IS group will send the offender an email warning. Tr. at 43.

unauthorized computer usage and the pattern of activity of the logs, the IS group concluded in September 2002 that the individual had intentionally accessed some of the sexually explicit material found under his user ID. *Id.* at 56.

3. The Individual's Cyber-security Expert

The individual presented the expert testimony of a police officer assigned to an Internet crime task force in a local jurisdiction. Tr. at 120. The expert offered explanations of how the SEAM could have appeared under the individual's user ID unintentionally. First, the expert testified that SEAM sites can send information to individual computers by "pop ups" and "pop unders." Tr. at 127. Backing out of a site that he did not intend to view could have triggered a SEAM "pop up" on the individual's computer. *Id.* at 128. Second, the expert argued that the small size of the pictures that the individual accessed (between three and six kilobytes) is similar to the size of thumbnail pictures that webmasters build onto their homepages to attract users to their sites. *Id.* at 129. This indicates to him that the individual looked at the thumbnail pictures, usually found on the first page of a website, and then backed out without accessing additional content. *Id.* at 130. Small websites could have been downloaded very quickly, and the log files reflect brief accesses. *Id.* Most downloaded pictures are around 200kb. *Id.* at 131. Third, the individual could have been "webjacked"- tricked into thinking that he was exiting a site by an "x" button that is hidden or is actually set up to open additional sites. *Id.* at 127-128. He could not have seen the sexually explicit pictures if they were behind the other websites that appeared by accidentally hyper linking on the first site. *Id.* at 127-135.

The expert also argued that the individual did not establish a pattern of accessing SEAM sites. *Id.* at 136-138. The expert disagreed with the DOE IS manager and concluded that "sextracker.com" was accessed on one day only, without any repeat visits. *Id.* at 137-139. The expert said that very little of the individual's unauthorized activity involved SEAM, and there was never a "pattern" established. *Id.* at 148. He considered a pattern to be "well over fifty thousand [pictures]." *Id.* Finally, the expert testified that, based on newsletters and his own investigations, SEAM sites are no more of a security risk than others. *Id.* at 151. He also argued that the DOE investigation was faulty, albeit through no fault of the IS manager. According to the expert, a proper investigation includes an interview of the individual to give the individual an opportunity to explain the presence of certain sites that appeared more than once in the log file. Tr. II at 7. He agreed that the log files that were entered into evidence did not provide enough information to determine the individual's activity. Tr. II at 8. The expert testified that had he conducted the forensic analysis, he would have used more sophisticated software with the ability to retrieve the Internet history from the hard drive itself and determine the amount of time that the individual spent on each site. Tr. at 131, 153.

4. Response of the DOE IS Manager

At the hearing, the DOE IS manager was provided the opportunity to address the expert's testimony. He agreed with the expert that it was possible for "pop ups" and "pop unders" to have caused the presence

of SEAM sites on the individual's files. Tr. at 157. He also admitted that DOE performed only a very basic forensic analysis because: (1) there was no indication of criminal activity and (2) the IS group was assigned only to flag violations of DOE policy, which at that time prohibited any personal use of government computers. *Id.* The manager explained that a higher level of analysis would have provided a complete record of the individual's Internet activity, including information about how much time the individual spent on a site and which sites he visited. Tr. at 163. This more detailed analysis would have allowed the IS group to recover information that may have been deleted by the system in normal usage. *Id.*

Nonetheless, the manager stressed that after he concluded that the individual had accessed unauthorized sites on a regular basis from April to August 2002, neither the individual nor his supervisor complained that the individual had not accessed those sites intentionally. *Id.* at 158. According to the IS manager, "nobody asked for any additional investigation because there didn't seem to be any dispute about the facts at the time." *Id.* He testified that although the expert's explanation was possible, he did not agree with the explanation and had not changed his opinion that some of the individual's activity was intentional. *Id.* He was skeptical about the individual's explanation such a long time after the report was issued. *Id.* at 159. The manager testified that if the individual had complained at the time the audit report was issued, the manager would have considered the alternate explanation a possibility. *Id.* However, the individual's reaction to the report at the time it was issued—not offering any explanation of how the material showed up under his user ID and not denying that he downloaded the pictures—confirmed the manager's suspicions that the individual was visiting the unauthorized sites intentionally. *Id.* at 160.

5. The Individual's Colleagues

Three of the individual's colleagues (including two managers) testified that the individual was an excellent, motivated employee and that they were eager to have him return to work. Tr. at 173, 215, 219, 220. They were uniform in their praise for the individual's honesty, dependability, excellence at performing his job, and reliability. Tr. at 200, 214-215, 219-221. They all said that they would trust him with their life, even in very dangerous situations. Tr. at 206, 214, 218. His managers also confirmed that the search on guns, firearm and fitness was work-related and approved by management as appropriate use of the computer. Tr. at 184, 213. In addition, they testified that the individual and his colleagues did not receive any training on the use of the Internet. *Id.* at 179-180, 211. They also testified that the employees in their office assumed that all computer usage was monitored by headquarters at all times. *Id.* at 181-184, 212. At the time of the discovery of the unauthorized material, the individual's manager wanted to treat the individual's unauthorized computer use as a disciplinary issue and not a security issue. *Id.* at 192. The individual was counseled immediately about proper use of the computer. *Id.* at 193-194, 196.

However, one of the individual's managers testified that the individual should have "self-reported" the appearance of unauthorized material on his computer screen, especially if it happened more than once. *Id.* at 202-203. He testified that other employees had reported to management or the IS group when they inadvertently accessed inappropriate material on the computer. *Id.* at 204. The manager testified that he

disciplined the individual not because of his access of unauthorized material, but rather because he had reported the activity “after the fact.” *Id.* at 202-203.

6. The Individual’s Wife

The individual’s wife testified that he had been very honest with her about the reason for his suspension from duty. Tr. at 168. She also maintained that he did not have any interest in pornography, and that their marriage was very happy and stable. Tr. at 168-169.

D. Evidence of Rehabilitation or Reformation

In previous cases, hearing officers have placed great weight on evidence of a new pattern of behavior to prove rehabilitation or reformation from the security concerns of Criterion G. *See Personnel Security Review*, OHA Case No. VSO-0122, 26 DOE ¶ 82,777 (1997), *affirmed* (OSA, July 31, 1997) (rehabilitation demonstrated by two years of government computer use without a new incident of unauthorized use); *Personnel Security Review*, OHA Case No. VSO-0435, 28 DOE ¶ 82,804 (2001), *affirmed* (OSA, October 2, 2001) (holding that insufficient time had passed since last unauthorized use to demonstrate rehabilitation or reformation from a pattern of unauthorized use of government computer). Although the passage of sufficient time could provide adequate evidence of reformation, at this time I am unable to determine the individual’s new pattern of behavior because he has been banned from the use of the Internet since September 2002, less than one year prior to the hearing in this case. ⁴

After reviewing the record in this case, I find that the individual has not adequately mitigated the concerns arising from his unauthorized use of a government computer. In reaching this conclusion, I found the testimony of the DOE IS manager to be both balanced and credible. The IS manager testified during the hearing that the process of detecting unauthorized computer use was an unpleasant part of his job, and he expressed empathy for the individual’s position. Tr. at 55, 162-163. He admitted the shortcomings of the basic forensic analysis that his staff conducted on the individual’s computer. *Id.* at 161. ⁵ Nonetheless,

4/ The record contains some evidence of mitigation. The individual and his colleagues credibly testified that they received inadequate training on the Internet and use of the computer. Based on the individual’s honesty with family and colleagues about his suspension, there is a low probability that the individual would be subject to coercion. The individual has also admitted his mistake, accepted responsibility for his actions, and in general exhibited a positive attitude throughout the process. Nonetheless, this is insufficient to mitigate DOE’s valid security concern about the individual’s judgment and unauthorized use of government computers.

5/ Both the DOE IS manager and the individual’s expert agreed that DOE’s forensic analysis of the individual’s computer did not provide sufficient detail to determine how long the individual actually spent on each unauthorized website, information which could support an inference as to his intent in visiting those sites. Even though both experts agree that they could not accurately discern the

(continued...)

the DOE manager steadfastly maintained that his original interpretation of the audit data was correct, and that some of the SEAM websites had been accessed intentionally. He gave a logical explanation, based on documentary evidence and past experience, of what he believed had transpired. Finally, even though the DOE IS manager ultimately rejected the theory of the individual's expert, he appeared to thoughtfully consider the opinion of that expert in arriving at his own conclusion.

In addition, the individual himself admitted that he showed poor judgment in his unauthorized computer usage. He has not denied that he accessed some SEAM sites over a period of four to five months after signing two agreements to restrict his use of the computer to government business only. ⁶ He admitted wasting time on other things besides surfing the Internet at a time when his office had a zero tolerance policy towards personal use of the Internet. Ex. 18, 20. Further, the individual did not report the recurring appearance of sexually explicit material on his computer or ask for help in avoiding material that a reasonable person would consider inappropriate, but instead continued accessing SEAM websites until he was discovered in August 2002. The individual accessed a type of website (adult or sexually explicit material) that DOE security considers at high risk of carrying malicious code, collecting information about users, and scanning computers for exploitable vulnerabilities. Despite this activity, the individual told the psychologist in October 2002 that he was "kind of surprised" when he got in trouble, causing the psychologist to recommend personalized training in computer security for the individual "[i]n light of [the individual's] attitude that [the individual] did not feel like he had done anything wrong." Ex. 21 at 3. ⁷ That

5/ (...continued)

individual's intentions using the available evidence, some conclusions can be drawn. This is not a criminal matter in which the government bears the burden of proving an individual guilty beyond a reasonable doubt. *See Personnel Security Review*, OHA Case No. VSO-0078, 25 DOE ¶ 82,802 (1996). In a DOE administrative review proceeding under Part 710, the burden is on the individual to provide evidence to convince the DOE that granting or restoring his access authorization "would not endanger the common defense and security and would be clearly consistent with the national interest." 10 C.F.R. § 710.27(d).

6/ In his defense, the individual draws my attention to OHA Case No. VSO-0122, 26 DOE ¶ 82,777 (1997), *affirmed* (OSA, July 31, 1997), arguing that the hearing officer recommended restoring the security clearance of a DOE contractor employee with an unstable marriage who admitted to intentionally downloading SEAM on his office computer for a period of two to three years. Tr. at 15-16. The individual contends that his actions in this case are much less egregious. *Id.* I find that Case No. VSO-0122 can be distinguished from the instant case. The contractor employee in Case No. VSO-0122 had last accessed SEAM two years prior to the hearing and while working for a previous employer, not the employer who requested his clearance. In fact, the previous employer had asked the contractor employee to resign because of his unauthorized computer use. The contractor employee was then hired by another contractor, and worked there for two years without any unauthorized use of his government computer.

7/ The psychologist was familiar with the individual and had evaluated him yearly since 1994. Ex. 21
(continued...)

attitude reflects a minimization of the seriousness of his actions in the context of DOE security concerns.

III. Conclusion

As explained in this Opinion, I find that the DOE Operations Office properly invoked 10 C.F.R. § 710.8 (g) and (l) in suspending the individual's access authorization. After being afforded ample opportunity, the individual has not, however, presented adequate mitigating factors that alleviate the legitimate security concerns of the DOE Operations Office. In view of these criteria and the record before me, I cannot find that restoring the individual's access authorization would not endanger the common defense and security and would be consistent with the national interest. Accordingly, I find that the individual's access authorization should not be restored.

Valerie Vance Adeyeye
Hearing Officer
Office of Hearings and Appeals

Date: February 18, 2004