* 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:	July 12, 2012	)	
		)	Case No.: PSH-12-0083
_____		)	

Issued: November 14, 2012

Hearing Officer Decision

William M. Schwartz, Hearing Officer:

This Decision considers the eligibility of XXXXXXXXXX (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, I find that 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 for at least 25 of his 27 years of employment. During a Personnel Security Interview on May 17, 2012, the individual admitted that he had failed to protect classified information properly on several occasions between 1988 and 2011, that he failed to report many of those incidents at the times they occurred, and that he received a written reprimand for several of those incidents.

Consequently, the local security office (LSO) issued the individual a Notification Letter in June 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

[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.

LSO explained that the derogatory information falls within the potentially disqualifying criteria in the security regulations at 10 C.F.R. § 710.8(g) and (l) (Criteria G and L).[2]

After the individual received the Notification Letter, he invoked his right to an administrative review hearing. Ex. 2. On July 13, 2012, the Director of the Office of Hearings and Appeals (OHA) appointed me as Hearing Officer, and I conducted the hearing. The DOE counsel introduced five numbered exhibits into the record, and the individual tendered six exhibits. The individual testified on his own behalf and called as witnesses his supervisor, a security incident specialist, and three co-workers.

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 G describes security concerns where an individual "violated or disregarded security or safeguards regulations to a degree which would be inconsistent with the national security; . . . or violated or disregarded regulations, procedures, or guidelines pertaining to classified or sensitive information technology systems." 10 C.F.R. § 710.8(g). 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

In its Notification Letter, the LSO supported its Criterion G security concern by alleging that the individual had demonstrated a pattern of failing to protect classified information and security violations. During a Personnel Security Interview (PSI) that was conducted on May 17, 2012, the individual admitted that he did the following from 1988 through 2010:

- In 1988, the individual left a classified document in his office, unprotected, when he went away to answer a colleague's question, though he was aware at the time that this action was contrary to company policy.[3]

- In 2003, the individual may have placed a classified document in his desk drawer when he went to use the restroom. While he does not recall the details surrounding the event, he admitted knowing that leaving a classified document unprotected was against company policy, and that he may have taken the document with him to the restroom.

- Although he had already been trained on how to properly post classified documents on SharePoint, in 2005, the individual posted a classified document to SharePoint without properly setting the document's viewing permissions.[4]

- In 2005, the individual failed to protect classified information when he left his office while viewing classified information on his computer. The individual failed to log off or lock his computer even though he had already been trained on handling classified information and knew that failure to protect classified information was against company policy.

- In 2009 or 2010, the individual improperly stored a highly classified document with other classified information, knowing that it violated company policy.

- In 2011, the individual e-mailed a highly classified document without encrypting it. Because his special classified access lapsed in January 2011, he may have been accessing highly classified information without authorization.

In 2012, the individual was given a written reprimand for failing to protect classified information and for failing to report these incidents in a timely manner. Later in 2012, he was also issued a security infraction for failing to report these incidents in a timely manner.

---

[3] The Notification Letter states that this event occurred in 1998. Ex. 1 at I.G. The individual corrected the date at the hearing, and the facts as reported in the PSI supports the individual's position. Transcript of Hearing (Tr.) at 33; Ex. 5 at 11.

[4] At the hearing, the individual clarified that the supporting software was not in fact SharePoint, but rather a comparable document-sharing program. Tr. at 31.

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

- In 2003, the individual brought his camera into a limited area and did not report the incident even though he was aware that it was against company policy.

- In early 2011, the individual brought his mp3 player into a limited area, twice in one day, and failed to report the incident, even though he was aware that it was against company policy.

- The individual admitted that on July 12, 2011, he failed a polygraph examination because he knew that he had mishandled classified information on numerous occasions and had not reported the incidents to security even though he was aware of the reporting requirements. He admitted that if he had not failed the polygraph examination, he would not have reported the security incidents.

The written reprimand and security infraction that were issued to the individual in 2012 were based in part on these incidents and his failure to report them in a timely manner.

Ex. 1.

I find that the above information constitutes derogatory information that raises questions about the individual's conduct under Criteria G and 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, ¶ 15. Further, noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems and the protection of classified information 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 Guidelines K at ¶ 33, M at ¶ 39.

IV. Findings of Fact

The individual has held a security clearance since at least 1987. Transcript of Hearing (Tr.) at 131. From 1987 until January 2011, the individual worked at the same position. *Id.* at 120. Due to the nature of their work, the individual and his co-workers handled classified documents constantly throughout the course of each work day. *Id.* at 131, 148. In January 2011, the individual assumed a new position that requires a less intensive interaction with classified material. *Id.* at 15.

The individual was selected for a random polygraph examination in July 2011. *Id.* at 52; Ex. 1. When the polygraph examiner asked him whether he had ever mishandled classified information, the testing indicated that the results were "inconclusive." Tr. at 15. The individual then recounted to the examiner two or three occasions on which he had mishandled classified information, but retesting again yielded inconclusive results.

Id. at 15, 58. The examiner suggested that the individual go home, try to recall all of the occasions on which he had made such errors, and then report them to security incident management program. *Id.* at 57.

After a sleepless night, the individual made a complete report to the appropriate security office, and later passed his polygraph examination. *Id.* at 16, 18.[5] He cooperated fully with the security office's investigation into the incidents he reported. *Id.* at 17, 86. Of the eight incidents described in the Notification Letter, the security investigation determined that three were minor events in which risk of compromise of classified information was deemed remote. *Id.* at 35, 37, 39, 62-63, 87. The remaining five incidents he reported were determined to be "non-incidents" or "near misses," that is, events that need not have been reported. *Id.* at 20, 26, 28, 31, 33.

Although the individual reported eight occasions on which he mishandled classified information or failed to comply with rules or policies about the protection of such information, with the exception of one occasion, he did not report the event immediately after it occurred. *Id.* at 25, 26 (did report immediately), 30, 32, 33, 35, 37, 39. I address each of these events below.

The oldest episode of mishandling classified information occurred in 1988. The individual explained at the hearing that he had only recently assumed a position that required intensive handling of classified documents, and he had not yet absorbed all of the rules and policies. *Id.* at 35. He left his office with classified information unattended; his office mate and mentor discovered the error, chastised him, but neither reported, nor encouraged the individual to report, the error to security. *Id.* at 34-35. When the security office investigated this incident in 2011, it determined that its impact on DOE security was relatively low—3 on a scale of 4, with 1 being the most serious and 4 being the least.[6] *Id.* at 62. The security office mitigated the concern for this event, finding that the information left out was not of particularly high classification level, that the event occurred within a protected area, and that the event was of short duration. *Id.* at 35.

The individual testified that he inadvertently brought his camera to work one day in 2003. He was having a home built at the time, and was recording its daily progress. He generally left the camera in his car, but for some unknown reason he had inadvertently slipped it into his jacket pocket that day. He did not discover the error until after work, when he found his camera in his pocket, which meant to him that it had been in the office all day. He did not report the event because he knew he had not used the camera in the

[5] The individual reported to the security office each of the eight events cited in the Notification Letter. He reported seven on the day after his polygraph examination. He reported the eighth only when he became aware that he might in fact have done something improper. That moment occurred after he had already received his notice of security infraction, which informed him that any future incidents could result in loss of employment. He nevertheless reported the event to his manager and to the security office. *Id.* at 25-26.

[6] The security investigation categorized each of the individual's reported events using an impact measurement index (IMI) number. This system of categorization was set forth in Section N of DOE's Manual 470.4-1. The Manual has since been replaced by Order 470.4b, which employs a different method of categorization of incidents, described at Attachment 5 of that directive.

office, and felt that no harm was done. After conducting its investigation in 2011, the security office determined that the possibility of compromise of security or classification matters was remote, and categorized the incident as IMI 3, similar to the 1988 incident. *Id.* at 38-40, 62.

The individual reported to the security incident investigator that he might have mishandled a classified document in 2003 by leaving it on his desk while he went to the bathroom. He could not remember the event well when he reported it in 2011, and stated that it was also possible that he had carried the document with him when he went to the bathroom. At the hearing, the individual had no clearer memory of the event, but stated that in 2003 they were permitted to carry documents with them to the bathroom. *Id.* at 32-33. The security incident investigator testified that he could find no evidence that the event even occurred, and deemed it a non-incident. He also stated that if the error had in fact occurred, he would nevertheless find it to be a non-reportable event, because it took place within a protected area. *Id.* at 91-92.

The individual also reported two occasions in 2005 when he recalled making errors that might have impacted the protection of classified information. In one instance, he was having a discussion in his office with a customer who worked for the same company (in-house customer). The discussion led him away from his office computer, which was operating in a classified mode, first to a table in his office, then ultimately out of the office. Distracted by the in-house customer, he neglected to sign off his computer, and realized upon returning that the computer had signed off automatically after ten minutes. *Id.* at 28-30. The second 2005 event concerned his sharing documents with co-workers through new computer software without setting proper restrictions on their availability. The individual reported that the in-house customer chastised him for his error. *Id.* at 31. At the hearing, the security investigator testified that he had interviewed the in-house customer, who is widely regarded for following security rules stringently. *Id.* at 90. The in-house customer had no recollection of these events, and if they had occurred as the individual reported, the security incident investigator was confident that the in-house customer would have reported it himself. *Id.* Consequently, the security incident investigator found no evidence that the events occurred, and deemed them to be non-incidents.

At the hearing, the individual testified that, during a routine review, in 2009 or 2010, of classified documents in his control, he discovered that he had some highly classified material, which should have been stored on a separate shelf, instead stored among other classified documents. He corrected the error, and duly reported the mistake to his office's classified administrative specialist, who appeared at the hearing and, after the polygraph examination, to the security office. *Id.* at 26-28. The specialist testified the error was "not a big deal" as all the shelves were appropriate storage locations for classified material, and the security investigation ultimately determined that it was a non-incident. *Id.* at 26, 106.

In 2011, after the individual had started in his new position, in a location where he was permitted to carry an mp3 player, he visited his old office, where such devices were not

allowed. After his visit, he realized that his mp3 player had been in his pocket during the visit. The security investigation found that any compromise of classified information was remote, and though the event was a reportable incident, it was categorized at IMI 4, the lowest level of concern. The individual stated that he no longer carries his mp3 player with him, but leaves it in his car, to avoid any future mistakes. He also stated that he did not report the incident at the time because, as with the camera in 2003, he knew that no harm had been done, though he acknowledged at the hearing that he should have reported it. *Id.* at 36-37, 62.

The final event the individual reported was also found to be a non-incident. His new position no longer required the special classified clearance that he had held in his former position, and that his special clearance had lapsed. Soon after he assumed his new position, he forwarded an encrypted e-mail message discussing a highly classified matter to a co-worker working on a similar topic. His first three attempts failed. He ultimately de-selected the encryption option and sent the message. He later learned that, though the intended recipient had the appropriate special clearance to view the material in the e-mail, his computer was not equipped to receive encrypted messages. At the PSI, one of the interviewers suggested that the individual may have mishandled classified information, because, in forwarding the e-mail, he accessed the highly classified information after his authorization to do so had expired. Acting on that suggestion, he reported the incident immediately following the PSI. After investigating this event, the security office determined that it, too, was a non-incident that need not have been reported, because the information contained in the e-mail message was not in fact of the highly classified type for which he no longer held authorization. *Id.* at 22-25.

V. Analysis

At the hearing, the individual's five witnesses offered their opinions concerning the individual's general adherence to security policy and the incidents that raised LSO's concerns. Each testified that the individual was a reliable, trustworthy employee who is very conscientious about protecting classified information. The security incident investigator stated that the individual was forthcoming in his self-report of all the occasions on which he believed he had mishandled classified material and that he had fully cooperated in the ensuing investigation. *Id.* at 86-88, 93. He pointed out that the individual was so thorough in reporting past events that he was unable to verify that two of them had even occurred. *Id.* at 89-92.

A co-worker testified that the individual was careful and organized when handling classified documents and, in his opinion, had better work habits in that regard than most of their co-workers, and models ideal behavior. *Id.* at 106, 109-10. A second co-worker, who has been the individual's colleague for 27 years, stated that the LSO's concerns were easy mistakes to make, and that neither he nor any of their co-workers has any concern about the individual's relationship with classified matter. *Id.* at 130, 132-34, 136. He further stated that the individual is very security-conscious, and that he trusts the individual with classified matters just as he trusts himself. *Id.* at 137-38, 144. A third co-worker offered similar observations, and pointed out that, when in a position to do so, the

individual took the extra precaution to clarify to others the rationale for certain information being classified, so that those working with the material would treat the information appropriately. *Id.* at 151.

The individual's current supervisor testified that the individual is very sensitive about classified material and, in his opinion, above average in handling it. *Id.* at 120. He issued the letter of reprimand to the individual, but did so only at the recommendation of their employer; he felt that, by the time the letter was issued, the individual had already learned his lesson and had reformed his behavior, including a willingness to report any future errors. *Id.* at 118, 124-26. He further stated that the individual has in fact reported security issues to him since the 2012 PSI. *Id.* at 11-17. He finds the individual to be very trustworthy and reliable, and has no concerns about the individual's future involvement with classified information. *Id.* at 119.

A. Criterion G concerns

The LSO identified six occasions, based on the individual's self-report, of mishandling classified information, as set forth in the Notification Letter and described above in Section III. The security office investigated each of these events, and determined that five of the six were best categorized as non-incidents. The investigation found no evidence that three of the five non-incidents occurred. Even if I assume that all five of them did in fact happen, none resulted in disclosures of classified information to unauthorized persons; obtaining, viewing or downloading such information outside one's need to know; or damage to the national security. Adjudicative Guidelines at Guideline K, ¶ 34(a), (d), (f), (i). On the other hand, while unintentional, they do constitute failures to comply with rules for the protection of classified information. *Id.* at ¶ 34(g). Nevertheless, I find that they, like the remaining concerns discussed below, occurred so infrequently in the span of the individual's 27-year employment, which includes 22 years of intensive handling of classified documents, and occurred under unusual circumstances not likely to recur, that they do not cast doubt on the individual's current reliability, trustworthiness, or good judgment. *Id.* at ¶ 35(a).

One of the six self-reported occasions was identified as a security incident, and formed a part of the factual basis for the letter of reprimand and security infraction notice the individual received in 2011. The security investigation found reduced concern for the individual's error—leaving his office with classified information unattended—because the information was not highly classified, was unattended for a short time, and was within a protected area. The individual's testimony offered additional factors that mitigate the LSO's concern: he committed this mistake in 1988, when he was new to the intensely classified environment and had not yet absorbed all the rules and policies, and his mentor, while aware of the mistake, did not encourage him to report it. A great deal of time has elapsed since this event, and he is no longer a newcomer to rules and policies for the protection of classified information. Moreover, as discussed below, the prevailing culture at the facility has slowly changed to an atmosphere that fosters reporting actual and potential threats to security systems, and the individual has demonstrated that he would

report such an event if one should arise in the future. Consequently, I find that the individual has mitigated the security concerns that arise from this incident. *Id.*

B. Criterion L concerns

Two of the factual bases for the LSO's concerns under Criterion L are occasions of unintentional noncompliance with rules—bringing a camera (2003) and an mp3 player (2011) into an area where such devices are not permitted. These occasions were also identified in the letter of reprimand and the notice of security infraction issued to the individual in 2011. The critical question is whether these two events, separated by eight years, demonstrate a pattern of behavior that raises issues of honesty, reliability, or trustworthiness. The individual testified about the unique circumstances under which each incident occurred, and they appear unlikely to recur. I further note that, because the individual was unaware in each instance that he had the proscribed items on his person, he did not touch them, let alone use them, while he was in areas from which they were prohibited. Therefore, as the security investigation concluded, the risk that his actions compromised any security measures was remote. I conclude that the individual has mitigated the LSO's concerns regarding these two events. Adjudicative Guidelines at Guideline M, ¶ 41(a).

Of equal if not greater concern under Criterion L is the individual's failure to report most of the events listed in the Notification Letter until after the 2011 polygraph. He produced testimony at the hearing, both his own and that of two long-time fellow employees of the same company, that the corporate culture in which they began their careers discouraged reporting or self-reporting breaches of rules for the protection of classified information, whether intentional or not. Tr. at 43, 121, 138 ("Three strikes and you're out"). This created an environment in which employees feared reporting or being reported, as their jobs would be in jeopardy, and one witness testified that the fear continues to some degree today. *Id.* at 154. That environment also encouraged employees to make their own judgment call as to whether a mistake caused any harm to the security and protection of classified information, and not to report if no harm was done. *Id.* at 153. Some employees continue to make their own judgment calls, though the culture is changing. *Id.* at 124-25. The individual also testified that he had had a bad experience working with security investigators in 1990, early in his career, that reinforced the culture of the time. *Id.* at 42, 79. Finally, the individual related insights he has gained from attending classes on human performance that he feels explain his failure to report. From those classes, he learned that people have a natural disinclination to admit mistakes, that they suspect they will be punished for their errors, and that they are skeptical of management's reaction to self-reporting. In the individual's situation, he contended, all these insights were reinforced by the corporate culture and his unfortunate prior experience with the security office. *Id.* at 43-45.

At the hearing, the individual testified about his current attitude toward security and the protection of classified information. The insight he gained from his human performance classes allowed him to analyze how his security errors occurred and how he can avoid repeating them. He determined that he makes mistakes when he does something (a) for

the first time, (b) in a new environment, (c) out of his normal routine, or (d) while interrupted by others. *Id.* at 48. He now recognizes that he must particularly vigilant when any of those conditions are present. He acknowledged that he will also need to exercise particular care if his clearance is restored to him, as he will be out of practice regarding compliance with all classification rules and policies. *Id.* at 49. He also testified that his recent involvement with the security investigation office has been a positive experience, despite the seriousness of the charges against him, and has taught him the importance of reporting any suspected breach of protocols. *Id.* at 66-67. That experience supports the security office's recent outreach to encourage employees to come forward and cooperate with their efforts. *Id.* at 46; Ex. E. The individual acknowledged that he should not be making the call, as he and others did in the past, whether any harm was done before deciding whether to report a potential problem to the security office. He now understands that he should report, and allow security to make that call. Tr. at 71. He has done so on a number of occasions since the PSI, and is committed to doing so in the future. *Id.* at 47, 49. Finally, he pointed out an additional incentive to be extremely careful in the future is warning contained in his reprimand letter; he knows that any further mishandling of classified information could subject him to dismissal. *Id.* at 47, 116. After considering this testimony, I find that the individual has mitigated the LSO's concerns regarding his past failure to report potential security issues.

Even though I have determined that the individual has mitigated each of the security concerns contained in the Notification Letter, the overarching concern is nevertheless whether the individual will act in the future in a manner that places the national security at risk. I consider the fact that, except in one instance, the individual did not report security mistakes under entirely voluntary conditions. Rather, he was having difficulty passing a polygraph examination, and was advised to make a full disclosure to security personnel. He did so, and later passed the polygraph examination. I note, however, that the individual has continued to report events that might impact security or protection of classified information. His willingness to report, even after he passed the polygraph examination and, more importantly, even after being placed on notice that future incidents could lead to his dismissal, demonstrates to me a changed frame of mind, one entirely in line with the attitude the LSO depends on to maintain and protect classified material.

The record in this case convinces me that the individual's self-reported history of security mistakes does not constitute a pattern of misconduct that predicts a similar future. Rather, it convinces me that his knowledge of security concerns is now stronger than ever, and taken together with the threat of dismissal for any future incidents and the humbling experience of this administrative review process, has raised his 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 mishandling of classified material and his honesty, reliability, and trustworthiness. *See Personnel Security Hearing*, Case No. PSH-12-0081 (2012) (similar security concerns mitigated).

VI. Conclusion

Because the individual has resolved the security concerns, 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: November 14, 2012