* 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-12-0081
		)	

Issued: October 11, 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 24 years. During a routine polygraph examination, the individual revealed that he had committed several errors handling classified information between 2000 and 2011 and failed to report them at the time they occurred. He also revealed that on three occasions between 2007 and 2012, he failed to comply with rules and procedures regarding conduct in limited access work areas. These admissions prompted the Local Security Office (LSO) to conduct a Personnel Security Interview (PSI) with the individual in January 2012. Ex. 7.

Because the PSI did not resolve the security concerns raised by the individual's admissions, the LSO issued the individual a Notification Letter in June 2012, advising him that it possessed reliable information that created a substantial doubt about his

[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.

eligibility to hold an access authorization. Ex. 1. In an attachment, the LSO explained that the derogatory information falls within the potentially disqualifying criteria in the security regulations at 10 C.F.R. § 710.8(f), (g), and (l) (Criteria F, G, and L).[2]

After the individual received the Notification Letter, he invoked his right to an administrative review hearing. Ex. 2. On July 5, 2012, the Director of the Office of Hearings and Appeals (OHA) appointed me Hearing Officer, and I conducted the hearing. The DOE counsel introduced seven numbered exhibits into the record, and the individual tendered one exhibit. The individual testified on his own behalf and called as witnesses his supervisor and two 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

[2] Criterion F concerns circumstances in which an individual "[d]eliberately misrepresented, falsified, or omitted significant information from a . . . Questionnaire for . . . National Security[] Positions . . ." 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." Finally, 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).

with the interests of national security" test indicates that "security clearance determinations should err, if they must, on the side of denials").

III. The Notification Letter and the Security Concerns

In its Notification Letter, the LSO supported its Criterion F security concern by alleging that the individual had provided it with false information. In the Questionnaire for National Security Positions (QNSP) he completed on April 24, 2009, the individual certified that in the past seven years, 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. However, during a Personnel Security Interview conducted on May 1, 2012, he admitted that he had put a classified disc into an unclassified computer.

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

- In 2000, the individual placed an unclassified computer disk into a machine that also contained a classified drive. He failed to report the incident to the Cyber Security office because he was scared and new to the department.

- On about five occasions in approximately 2000, the individual left classified material out on his desk unattended, and failed to report the incidents to security.

- On one occasion between 2000 and 2002, the individual left a classified hard drive out on a desk overnight, unsecured, and failed to report the incident to security.

- In 2006, the individual placed a disk containing classified information in his unclassified computer. He did not report the incident for two or three years, though he knew he was required to report it immediately.

- In approximately 2010, the individual left a safe that contained classified information open and unsecured for about an hour and a half.

- On one or two occasions between 2010 and 2011, the individual took classified information from a vault without properly protecting it, and failed to report the incident or incidents to security at the time of occurrence.

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

- On December 20, 2007, the individual brought his cell phone into an area of the facility in which cell phones are not permitted.

- In 2011, the individual left his computer, while connected to classified software, unattended and unlocked when he left his office to attend a meeting. He did not report the incident to Cyber Security.

- On two occasions in February and March 2012, the individual allowed a co-worker to "shadow" him through the access door into and out of their secured work area. He did not report the incidents as required.

- On March 12, 2012, during a random polygraph examination, the individual admitted to several of the above incidents.

Ex. 1.

I find that the above information constitutes derogatory information that raises questions about the individual's conduct under Criteria F, 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, ¶ 17. 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 ¶ 34, M at ¶ 39.

IV. Findings of Fact

The facts underlying the various incidents the individual reported are not in dispute, because the individual was the sole source of this derogatory information. I address each incident in detail in Section V below, where I discuss the individual's testimony at the hearing.[3]

The individual held a security clearance from 1982 to 1990 and has held one continuously since 1996. Transcript of Hearing (Tr.) at 122. In 1998, the individual began working at his current assignment. *Id.* at 125. Due to the nature of their work, the individual and his co-workers handle classified documents, along with unclassified material, constantly in the course of each work day. *Id.* at 101.

[3] As an initial matter, I note that the LSO refers to the individual's admissions of errors in handling classified material or failing to comply with security rules or procedures as "security incidents/violations" or "security violations." Ex. 1 at II.A, III.A, III.B. I take administrative notice of DOE Orders 470.4B and 471.1B, which discuss such terms as "violations" and "infractions." Incidents of security concern require inquiry and reporting in order to assign responsibility to an individual, who then may be issued a notice of infraction or violation. I have no reason to believe that the LSO charged the individual with an infraction or violation at any time. As a result, I conclude that the LSO was inaccurate in characterizing the behavior the individual admitted to as such, and has employed the terms "violation" and "incident" in their non-technical senses.

When the individual learned that he had been randomly selected for a polygraph examination, he surmised that he would be questioned about his protection of classified material and, in preparation for the hearing, forced himself to recall every possible error he had made while handling classified documents. *Id.* at 136-37. After he discussed these errors with the polygraph examiner, the examiner reported them to the LSO. Exhibit 4. At the subsequent Personnel Security Interview, the individual provided additional details regarding these errors, and admitted to other incidents, cited above, in which he had also improperly handled classified material or failed to follow procedures designed to protect such material, such as allowing his co-worker to "shadow" him. Exhibit 7 (Transcript of Personnel Security Interview, January 12, 2012). Nothing in the record indicates that the LSO, once informed of these incidents, issued any formal notice of security violation, infraction or incident arising from the reported information.

V. Analysis

At the hearing, the individual's three witnesses offered their opinions concerning the individual's general adherence to security policy and the incidents that raised LSO's concerns. The individual's supervisor testified that the individual has a positive attitude toward protecting classified information: he is careful and serious about his responsibilities, he makes suggestions to improve office procedures in that area, raises security issues at daily staff meetings, helps new staff members understand those procedures, and has invited cyber security personnel to speak to the office staff. Tr. at 13-15, 41, 44. The supervisor stated that, until the position was recently abolished, the individual had special duties as the custodian of classified removable electronic media (CREM) for the department and handled those duties well. *Id.* at 12, 28. Despite the number of security mistakes the individual admitted to, the supervisor finds these errors to be isolated, spread over several years, and not indicative of a pattern of willful or negligent disregard for rules. *Id.* at 15.

A co-worker testified that he has worked with the individual since 1998. *Id.* at 46. He stated that, until the office was converted into a secured area, they used to watch each other's classified material when one needed to step away from it temporarily. *Id.* at 47. He testified that the individual is honest, reliable and trustworthy and, despite the security concerns, can be counted on to follow rules. *Id.* at 47. He stated that over the years the office has been subject to hardware and software changes that have required modification of security procedures, and acknowledged a learning curve for these changes. *Id.* at 48, 50. He also stated that it was the individual who has asked Cyber Security personnel to provide training to the office in these circumstances. *Id.* at 51. Like the supervisor, this witness did not believe the individual's security errors constituted a worrisome pattern of conduct, and pointed out that the individual has taken full responsibilities for those errors. *Id.* at 60-61.

The third witness has worked with the individual for 20 years and performs internal audits that include assessments of security practices regarding classified information. *Id.* at 73-74. He stated that the individual generally exhibits care and concern in his handling of classified material. *Id.* at 78. He noted that the individual works with classified

information much more often than most cleared personnel, and so the risk of error is much greater for him. He further testified that many of the LSO's concerns consist of minor errors, and in any event do not represent how the individual generally handles classified information. *Id.* at 79. He also pointed out that many of the errors occurred early in the individual's tenure at his current position, and stated that it is typically difficult at their facility to get advice on handling classified material. *Id.* at 88. Finally, he stated, as the individual did later in the hearing, that anyone who has handled classified information as much as the individual, and for as long a period, if he were honest with himself and delved deep into his memory, would produce a similarly lengthy list of mistakes made. *Id.* at 90, 93, 103.

A. Criterion F concerns

The individual addressed each of the LSO's concerns. The LSO's basis for its Criterion F concern was the allegation that he had deliberately misrepresented significant information: he stated on his 2009 QNSP that he had never introduced unauthorized media into a computer system when specifically prohibited by rules or regulations, though he admitted in 2011 and 2012 that he had inserted a classified disk into his unclassified computer in 2006. He has consistently explained that this was a new question on the 2009 QNSP and he misinterpreted it to be narrowly inquiring about intentional, unauthorized actions outside of the facility. *Id.* at 105-06; Exhibit 7 at 74. He did not believe that it applied to the mistake he made in 2006, when he inserted a classified disk into his unclassified computer at his work station. At the hearing, he convincingly argued that he had no intention to mislead the LSO with his response on the QNSP. He explained that, as the result of security training he received some two years after this mistake occurred, he realized that he should have reported the episode. Tr. at 128. Immediately after the training in 2008, he conferred with his supervisor, who accompanied him to Cyber Security to file a report, and Cyber Security subsequently sanitized his computer. *Id.* at 53-54 (testimony of co-worker), 111. Therefore, Cyber Security was already aware of the 2006 event by the time he completed his QNSP in 2009. This fact, he contended at the hearing, supports his assertion that his incorrect response on the QNSP resulted from his misunderstanding the question rather than from a deliberate attempt to hide derogatory information from the LSO. *Id.* at 112-13. Moreover, he has spoken with his employer's security department about the misinterpretation, and is committed to seek its help "if I ever have a doubt of understanding on the questionnaire in the future." *Id.* at 113.

Based on my evaluation of the individual's demeanor and my assessment of his credibility, I find that the individual did not deliberately omit information from his 2009 QNSP. For this reason, I find that the individual has mitigated the security concern associated with Criterion F. *See Personnel Security Hearing*, Case No. TSO-0983 (March 24, 2011) (Criterion F concern mitigated where requisite element of "deliberateness" is lacking).[4]

[4] Decisions issued by the Office of Hearings and Appeals (OHA) are available on the OHA website located at http://www.oha.doe.gov. The text of a cited decision may be accessed by entering the case number of the decision in the search engine located at http://www.oha.doe.gov/search.htm.

B. Criterion G concerns

Three of the individual's mistakes occurred between 2000 and 2002, shortly after he began working in his current position. *Id.* at 124-25. He testified that there were many procedures to master for handling classified information in that office, and "it was hard to get any help." *Id.* at 124. He believed he had informed his supervisor when he left the classified hard drive out overnight, and recalled that he and his supervisor had determined that no compromise had occurred and that the event need not be reported. *Id.* Regarding those occasions when he had left classified material on his desk unattended, the individual's recollection was that these were times when he left his room to go to a neighboring room, realized his error and returned immediately to correct the error. *Id.* at 144. On each of those occasions between 2000 and 2002, he decided on his own that there had been no compromise and did not report the error. *Id.* at 143. Similarly, in 2000, the individual placed an unclassified computer disk into a machine that also contained a classified drive. In this situation he also determined that no information had been compromised, and admitted that he was afraid to admit the mistake to Cyber Security. *Id.* at 142. The individual testified that none of these mistakes can recur, both because their computing technology has changed such that they cannot insert unclassified media into classified systems and because, in 2011, the office was transformed into a closed, secured area, where many of the previous procedures for protecting classified material are no longer necessary and are no longer in effect. *Id.* at 111, 133. More important is the testimony of both the individual and his long-time co-worker that little training was provided in the protection of classified material, and the security training they did receive did not address all the requirements of their department. *Id.* at 51. The individual's years of experience in his office have given him the requisite knowledge for handling classified material, and his track record since those early years, while not unblemished, demonstrates an acquired sensitivity and proactivity toward properly handling such information.[5] Consequently, I find that the individual's current mindset, as well an improved working environment, mitigate these early mistakes. In reaching this conclusion, I have considered the mitigating conditions of Guideline K of the Adjudicative Guidelines.[6] The record establishes that the behavior occurred long ago and

---

[5] I note also that, though the LSO is now fully aware of these errors, it has not taken any action against the individual, such as charging him with a security infraction or violation, for committing these errors nor, for that matter, any of the matters listed in the Notification Letter.

[6] Guideline K 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 individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and
>
> (c) the security violations were due to improper or inadequate training.

Id. at Guideline K, ¶ 35.

under circumstances such that it is not likely to recur, and that inadequate training may have contributed to the errors. Guideline K at ¶ 35(a), (c).

In 2006, the individual placed a classified disk in his unclassified computer "because it was easier to view." Exhibit 1 at II.D. (This is the same error discussed above regarding the Criterion F concern.) At his PSI, he explained that he realized his error and removed the disk from the computer, where it had been for no more than 15 seconds. Exhibit 7 at 27. He also explained at both the PSI and the hearing that the process for viewing a file was easier on his unclassified computer than on his classified computer, but that was not the reason he acted improperly; rather, he had acted in haste and had not realized that the disk was classified until after he had inserted it into the wrong computer. *Id.* at 31-32; Tr. at 126-27. As stated above, he reported the event about two years later, immediately after receiving training that caused him to determine that it was a reportable event. Tr. at 128. Cyber Security concluded that there had been no compromise of classified information, and no action was taken against the individual for his error. Exhibit 7 at 38, 40, 42. At the hearing, he testified that, due to technological advances in the office, this error can no longer recur. Tr. at 128, 132. He also testified, as set forth above, that it was training he received in 2008 that made him realize that he needed to report this 2006 event. Once again, while it is important to consider that the work environment has been modified so that this error cannot recur, more important is that the individual responded favorably to security training in 2008. Furthermore, he demonstrates a positive attitude toward eliminating security mistakes by raising questions at daily safety and security meetings and seeking clarification from Cyber Security for himself, his co-workers, and newly hired personnel. *Id.* at 13-14, 41-42 (testimony of supervisor), 115, 117. *See* Guideline K at ¶ 35(a), (b), (c). I therefore find that the individual has mitigated the LSO's concern that this event raised.

The individual also stated during his PSI that in 2010, he had left a safe containing classified information open for about an hour and a half. He admitted that he had become distracted just as he was leaving the safe and neglected to set the handle in the locked position. He reported the error to his supervisor and Cyber Security immediately upon realizing what had happened. No material was found to be missing or compromised, and no action was taken against the individual for his error. Exhibit 7 at 84-90. At the hearing, the individual's supervisor as well as the individual stated that this error cannot recur due to the office's reconfiguration as a secured area. Tr. at 13, 114. This event appears to be one of pure inattention. While such negligence is not to be condoned, this behavior was isolated, particularly when one considers that the safe was the repository for his department's CREM, over which the individual had responsibility for several years. *Id.* at 113-14; Exhibit A (Statement of Co-Worker). Given that the event is highly unlikely to recur, not only due to the reconfiguration of the work area, but also due to the isolated nature of the event, I do not find that this error casts doubt on the individual's reliability, trustworthiness or good judgment, and further find that he has mitigated the LSO's concern in this regard. *See* Guideline K at ¶ 35(a).

At his PSI, the individual stated that once or twice in 2010 or 2011, he carried classified information out of his office without properly protecting it. He explained that he often

deletes classified information from a document and carries the redacted version to a classification expert who will review the document to ensure that it no longer contains any classified information. It was such a document that he, on one or two occasions, failed to insert into the proper protective cover before he stepped out of his office. On those occasions, he completed those steps as he had passed into the hallway. Exhibit 7 at 67-73. At the hearing, he testified that he had not considered what he did a security incident until he took the time to review all of his handling of classified information in preparation for the polygraph examination in 2012. As a result, he did not report these events to security at the time. Tr. at 140. These events arose from poor timing and he corrected them instantly. Had the individual paused to complete the covering of the documents before he stepped into the hall, his actions would have been proper. He did not, however, and therefore they raise a legitimate concern. Nevertheless, I consider these errors to be minor. Moreover, once the individual realized what he had done, through his introspection before and during his polygraph examination, he acknowledged them as errors and reported them to the examiner. My assessment of the individual and his conduct throughout this proceeding convinces me that that session of introspection has further heightened his awareness of security matters, and that he has since been more vigilant about the details of protecting classified information. I therefore find that the individual has mitigated this concern.

C. Criterion L concerns

In 2007, the individual brought his cell phone into his work area, where cell phones were prohibited. At his PSI and at the hearing, he convincingly explained that the circumstances surrounding that event were highly unusual. He was leaving for work with his hands full, as he was transporting supplies for an office party, and his wife slipped his cell into a pocket for him, which was contrary to his daily routine. When he reached work, he took off his coat and discovered the phone in his pocket. He immediately brought the phone to a guard, who confiscated it, had it examined, and returned it to him later in the day. Exhibit 7 at 91, 96-97, Tr. at 129-30. He also reported the event to his co-workers at the daily meeting, to remind others not to be careless. Tr. at 118. No disciplinary action or security infraction was issued at the time, and the incident has never been repeated. Tr. at 129. From the testimony, I can only conclude that carrying his cell phone into his work area was an unintentional, isolated incident. Not only did he react appropriately upon discovering his mistake, but he has not repeated the error in the five years that have passed since it happened. Guideline M of the Adjudicative Guidelines addresses use of information technology systems and, similar to Guideline K, provide examples of behavior that may mitigate security concerns of this type.[7] After

[7] 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

considering the mitigating conditions listed in that guideline, I find that the individual has mitigated the LSO's security concern, because the behavior happened long ago and under circumstances not likely to recur, it was inadvertent, and was followed by a good-faith effort to correct the situation by notifying the appropriate authorities. *See* Guideline M at ¶ 41(a), (c).

In 2011, the individual left classified software running on his computer when he was called into a meeting nearby, within the secured area that had recently been created. The software had recently been installed and the staff had not yet received training on its use. As he entered the meeting, he approached his supervisor and informed him that he had left the software running. The supervisor advised him to return to his office and take specified action to secure his computer, which he did. At the hearing, the supervisor testified that the individual did not know the rules for handling the software at the time of the incident, that he was proactive by raising his concerns in front of those assembled for the meeting, and that he had handled the situation properly. *Id.* at 14, 30-31, 34, 36-37, 110-11, 145. The supervisor also stated that the individual reporting to him was sufficient, that no security breach had occurred, and that the individual need not report the event to Cyber Security. *Id.* at 25, 38. Factors that mitigate the LSO's concern include, first, that the individual had not yet been trained in the proper security procedures for the new software and second, that he was following his supervisor's instructions when he did not report the error outside his office. *See* Guideline M at ¶ 41(a), (c).

The final, and most recent, event that raises a security concern occurred when the individual assisted a co-worker, who held the appropriate security clearances, to enter the secured area in which they work when the latter's security badge was not functioning properly. The co-worker testified at the hearing, stating that he did not believe it was improper for the individual to help him enter the area in which they both worked. Tr. at 65. He admitted, however, that neither he nor the individual knew the security rules that governed this behavior. *Id.* at 69-70. Another witness, who enters the individual's work area as a visitor, testified that the individual follows the proper protocol for admitting visitors. *Id.* at 75. The co-worker explained at the hearing that the individual let the co-worker through the access point twice, but after the second time he advised the co-worker that he was not comfortable about the activity and that he should report that his badge was not functioning properly. *Id.* at 69. Under these circumstances, the individual was acting intentionally. Nevertheless, he quickly realized the possibility that his behavior, however helpful to his co-worker and the efficiency of his office's operations, was possibly not in compliance with proper procedure. Although he did not report the activity himself, he did refuse to continue assisting his co-worker and enjoined him to report the problem. While his delay in addressing a procedural irregularity clearly raises

---

(cont'd)

(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.

a security concern, I find that mitigating factors include the individual's knowledge that his co-worker of several years had the authority to enter their common work area, *id.* at 66, and a contemporaneous realization that the situation needed to be addressed and corrected. Although these mitigating factors are not listed at Guideline M, I believe that a common-sense approach to determining the seriousness of the individual's transgressions argues for some leniency under these circumstances. Consequently, I find that the individual has mitigated the LSO's security concerns about this incident.

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 the individual did not report his past security mistakes under entirely voluntary conditions. He was facing a polygraph examination and wanted to pass it. A reasonable person would conclude that he might not pass the examination unless he was completely truthful. Nevertheless, I note that the individual divulged additional derogatory information at his PSI, following the polygraph examination, which he did pass. His willingness to provide complete information to the LSO even after he had passed the polygraph examination 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.

While the Notification Letter raised a significant number of security concerns, I take note that these concerns occurred over a period of 12 years, during which time the individual handled, in his estimate, tens of thousands of classified documents. Tr. at 101-02. After considering all of the evidence before me, I see the individual's compliance with the rules and procedures for protecting classified material and using information technology systems as one of gradual improvement. He admitted that, when he first began handling classified material intensively in his new position in 1998, he was not familiar with the rules, had difficulty getting the instruction he needed, and feared admitting his mistakes. Over time, he gained knowledge, mainly through on-the-job experience, but also through training, such as the 2008 session that made him realize an error he made in 2006. Since then, he acknowledges errors as he realizes them, seeks out instruction from knowledgeable sources, including Cyber Security, raises potential issues at daily safety and security meetings, and serves as the "go-to guy" in his office on these matters. *See* Attachment A. The record in this case has convinced me that the individual's self-admitted past 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 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 mistakes regarding handling of classified material, his noncompliance with rules pertaining to information technology systems, and his honesty, reliability and trustworthiness.

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: October 11, 2012