United States Department of Energy
Office of Hearings and Appeals

In the Matter of:	Personnel Security Hearing	)	
		)	
Filing Date:	July 26, 2012	)	
		)	Case No.: PSH-12-0098
		)	

Issued:

Hearing Officer Decision

Richard A. Cronin, Jr., Hearing Officer:

This Decision concerns the eligibility of XXXXXXXXXXXXXXXX ("the Individual") to hold a Department of Energy (DOE) access authorization.[1] For the reasons detailed below, I find that the Individual's suspended access authorization should be restored.

I. BACKGROUND

The Individual is a contractor employee at a DOE facility who has possessed a security clearance since 1979. Exhibit (Ex.) 10 at 43. In January 2012, the Local Security Office (LSO) received an incident report indicating that the Individual had received a security infraction for failure to protect classified information. Ex. 7 at 1; Ex 3 at 1. The incident report also disclosed that the Individual had committed other security rule violations that the Individual had not previously reported. Ex. 7 at 1. The LSO subsequently conducted a personnel security interview with the Individual in March 2012 (2012 PSI). Ex. 9.

Because the 2012 PSI did not resolve the concerns raised by the Individual's security rule violations, the LSO informed the Individual in a June 2012 notification letter (Notification Letter) that derogatory information existed under 10 C.F.R. § 710.8 (g) and (l) (Criterion G and L, respectively) that created a substantial doubt as to his eligibility to retain a security clearance.[2]

[1] 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.

[2] Criterion G pertains to information indicating that an individual has "[f]ailed 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; or violated or disregarded regulations, procedures, or guidelines pertaining to classified or

Ex. 1. The Notification Letter also informed the Individual that his security clearance was suspended and he was entitled to a hearing before a Hearing Officer in order to resolve the security concerns. *Id*.

The Individual requested a hearing on this matter. At the hearing, the DOE counsel introduced 10 exhibits into the record (Exs. 1-10). The Individual presented his own testimony, as well as the testimony of a former supervisor (Former Supervisor), and the team lead (Team Lead) from his employer's security incident office's (SIO) inquiry team. *See* Transcript of Hearing, Case No. PSH-12-0098 (hereinafter cited as "Tr"). The Individual also submitted four exhibits. (Ex. A-D).

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*; s*ee generally Dep't of the Navy v. Egan*, 484 U.S. 518, 531 (1988) (*Egan*) (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").

III. DEROGATORY INFORMATION AND SECURITY CONCERNS

To support its Criterion G and L concerns, the LSO cites a number of security violations that the Individual admitted to during the 2012 PSI. These violations range from inadvertently taking

---

sensitive information technology systems." 10 C.F.R. § 710.8(g). Criterion L concerns conduct tending to show that the Individual was "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." 10 C.F.R. § 710.8(l).

classified documents to his hotel room to using an unauthorized hard drive in non-classified computer systems. Further, the Individual did not report most of the incidents to security officials. Deliberate or negligent failure to comply with rules and regulations for protecting sensitive systems, networks, and classified information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern. *See* A*djudicative Guidelines*, Guideline M, ¶ 39; *Adjudicative Guidelines* Guideline E, ¶ 15; s*ee also, e.g., Personnel Security Hearing*, Case No. PSH-12-0081 (2012). In light of the Individual's admissions regarding his failure to comply with classified information protection rules and classified computer system rules and procedures, I find that the LSO properly invoked Criteria G and L.

IV. FINDINGS OF FACT

In April 2011, the facility administered a polygraph test to the Individual and the test indicated an inconclusive result regarding one question. Ex. 9 at 33-34. The Individual informed the polygraph examiner that he believed that this result was caused by his failure to report several prior security incidents involving classified information to the SIO. Ex. 9 at 33. The Individual later reported his prior security violations to the SIO. Ex. 9 at 33-34. After meeting with SIO officials, the Individual disclosed additional security incidents. Because of his disclosures, in January 2012, the SIO issued the Individual a "security infraction."[3] Additionally, the Individual received a verbal reprimand. These actions were based on the Individual's failure to report security incidents regarding classified information, and for being at fault for a security incident during the previous 24-month period.[4] Ex. 7 at 1.

During the 2012 PSI, the Individual described the following security incidents:

- During 2010 to 2011, the Individual improperly stored his password to a classified computer system by locking it in his desk drawer (Password Incident).
- During 2007 to 2011, the Individual used a personal thumb drive on approximately 20 occasions (Thumb Drive Incidents) to store Official Use Only, Unclassified Controlled Nuclear Information, and Classified Foreign Government Information. Ex. 9 at 102-04.[5]
- In two separate meetings during 2009, the Individual inadvertently placed classified documents in his briefcase (Document Incidents) and took the

[3] See *infra* regarding the definition of a security infraction.

[4]The Notification Letter references that the Individual received a written reprimand. This allegation is based upon the Individual's admission that he believed that he received a written reprimand when he signed a document. Ex. 9 at 149. However, upon reviewing the record, the formal security infraction document that the Individual signed only references a verbal reprimand. *See* Ex. 7 at 2. Given the evidence before me and despite the Individual's apparent admission in the 2012 PSI, I do not believe that the Individual received a written reprimand for his security errors.

[5] The Notification Letter states that the Individual admitted that, when he used the thumb drives, the Individual knew of the policy against such use. However, upon examination of the 2012 PSI transcript, the Individual immediately clarified his admission by stating that he was not sure that he was, in fact, aware of the policy. Ex. 9 at 108.

documents back to his hotel room on both occasions. The Individual returned the documents the next morning to the facility where the meetings took place. Ex. 9 at 14.

- From 1994 to 2011, the Individual stored a possibly classified Excel file on his unclassified workplace computer (Excel File Incident). Ex. 9 at 14. Individual admitted that when he created the file he should have had a derivative classifier review the file but failed to do so. Ex. 9 at 94-96.

Further, the Individual did not report any of these errors until after his polygraph test.[6] Ex. 9 at 16, 19-20, 23, 43, 69-70, 77-79, 81, 147.

Additionally, during the 2012 PSI, the Individual admitted to the following security incidents[7]:

- He had failed to properly handle and protect classified information and did not report these incidents to the SIO as required.
- Between 1994 and 2011, he intentionally did not report his security errors that occurred because he was ashamed, embarrassed, and afraid of the consequences if he reported the errors. Ex. 9 at 23, 28. Additionally, the Individual admitted that his failure to report the security incidents could have been used for blackmail. Ex. 9 at 23, 43, 69-70, 79, 147.
- He had taken personal thumb drives into a Sensitive Compartmented Information Facility (SCIF) on five occasions despite knowing that bringing the drives in the SCIF violated his employer's policies (SCIF Thumb Drive Incidents) and that he did not report the incidents because he was afraid of the consequences. Ex. 9 at 64-70.
- On two occasions, once in 2009 and once in 2010, the Individual took a personal cell phone into a security area to attend a meeting (Cell Phone Incidents). On both occasions, he discovered that he was carrying his personal cell phone but did not leave the meetings to remove the cell phone. Ex. 9 at 72-82. The Individual admitted while he reported the first incident to the SIO, that he did not report the 2010 incident because he believed he would be issued a security infraction. Ex. 9 at 77, 81.
- During the period 2006 to 2009, he had connected a personal back-up hard drive to a facility computer (Hard Drive Incident). Ex. 9 at 47-48.[8]
- In 2003, he entered data into an unclassified system (Data Incident) believing that such an entry of data would make the data already existing in the computer classified. The Individual admitted that he entered the data, despite feeling uncomfortable doing so, because of pressure from co-workers. Ex. 9 at 82-85.

[6] The Notification Letter cited this information as Criterion G derogatory information.

[7] The Notification Letter cited this information, along with the previously described Criterion G information, as Criterion L derogatory information.

[8] The Notification Letter alleges that the Individual stated in the PSI that he knew his use of the Hard Drive violated security rules. However, in the 2012 PSI, the Individual stated that he was unsure if the facility had instituted rules prohibiting their use. Ex. 9 at 47.

V. MITIGATION

At the hearing, the Individual presented witnesses in an attempt to establish that many of the security errors arose from inadvertent mistakes and not from a deliberate intent to violate security rules and regulations, and that he voluntarily reported the errors to the SIO after his polygraph test. He also seeks to establish that the failure to comply with the rules constitutes an isolated and infrequent pattern of conduct. The Individual asserts that the most serious failure represented by the Criterion G and L concerns is not notifying responsible officials of his security errors. In this regard the Individual presented testimony to establish that his attitude toward compliance with security incident reporting requirements is totally different as a result of the consequences of his errors, his work in creating a root-cause analysis of his security failures, his conducting a "lessons learned" presentation to his co-workers, and the extra measures he has taken to ensure future compliance.

A. The Individual's Testimony

The Individual testified that when he took the polygraph test in April 2011, the examiner informed him that the test indicated "something here" with regard to the Individual's answer whether he had ever provided information to foreign groups. Tr. at 18. The Individual told the examiner that "something came into [his] mind" when he was asked that question and informed the examiner that he had remembered that he had inadvertently mishandled classified information at an off-site secured meeting facility. Tr. at 18. Additionally, the Individual informed the examiner about the Data Incident. Tr. at 19. Despite his statement to the contrary at the 2012 PSI, the Individual was never informed that he failed the polygraph test.[9] Tr. at 20; *see* note 15, *infra*.

After the April 2011 polygraph test, the Individual went to the facility's SIO to report the incidents he had recounted to the polygraph examiner. Tr. at 21-23. Several days later, the Individual began to recall other incidents (SCIF Thumb Drive Incidents and Cell Phone Incidents) where he had not followed security regulations and he then reported these incidents to the SIO. Tr. at 23. Eventually, the Individual recalled all of the incidents listed in the Notification Letter and informed the SIO. Tr. at 27. The Individual is unable to recall any other security incidents occurring over his 30-year career. Tr. at 28.

With regard to the incidents described in the Notification Letter, the Individual testified that the Password Incident involved a password to a software application on a classified computer system. Tr. at 41. The Individual testified that he did not receive any formal training regarding the procedure to store the password.[10] Tr. at 45-46. When the Individual verbally received the password, he asked other co-workers about the best way to store the password. Tr. at 44. The co-workers informed him that he should store the password on the classified computer itself. Tr. at

[9] The facility administered another polygraph test of the Individual in the summer of 2011 but, as of the date of the hearing, has yet to receive the results. Tr. at 21.

[10] The Individual's password was active for six months. Tr. at 46.

44. Using his own training, the Individual determined his co-workers were wrong because storing the password on the system itself was insecure if the computer's security was breached. Tr. at 44-46. The Individual now knows that he should have consulted a computer security representative about the proper method of storage should have been and how to protect a classified password. Tr. at 47, 49.

The Individual testified that his use of personal thumb drives and a personal hard drive (Thumb Drive and Hard Drive Incidents) were for solely work-related purposes. Tr. at 53. He treated the thumb drives and the hard drive as if they were government-issued equipment and kept personal control over the equipment. Tr. at 53. None of the computer files he moved or stored with these drives were classified nor did he ever connect the devices to any classified computer system. Tr. at 54. The Individual testified that at the time he purchased the drives he was not aware of any policy prohibiting him from using such drives at his employment. Tr. at 55. Later, after he purchased the drives, he received computer-based training informing him that he could not bring "personal items" into the area where he worked. Tr. at 55-56. He did not immediately realize that this policy would prohibit him from using these drives because he had always treated them as "government-issued," and as such he kept the drives under secure procedures and did not connect the drives to classified systems. Tr. at 56. When officials asked employees to put encryption software on drives, he put such software on the personal drives he was using. Tr. at 56. The Individual stopped using these drives when his employer issued employees special protected flash drives.[11] Tr. at 57.

With regard to the Document Incidents, the Individual testified that on both occasions, in 2009, he was attending a multi-day meeting at a secure location. In both meetings, he inadvertently took classified documents to his hotel room. Tr. at 77. Both multi-day meeting locations had a table with numerous documents upon it, both classified and non-classified documents. Tr. at 66, 71. When he gathered up documents he brought to the meetings he inadvertently gathered up classified documents. Tr. at 67, 72. After realizing he had possession of the classified documents, he returned the documents the next day where he had obtained the documents. Tr. at 68-69, 72. The Individual testified that he did not report these incidents because he was embarrassed and afraid that he would be removed from the project he was working on. Tr. at 74. He is confident that this type of incident would never happen again because as a result of his root-cause analysis he now asks about the security situation when he goes to a new facility. Tr. at 76. In his 30 year career, the Individual had never mishandled a classified document other than on these two occasions in 2009. Tr. at 77.

In reference to the Excel File Incident, the Individual testified that, in 1994, he was working on a project and, as a product of his work, he created an Excel spreadsheet file. Tr. at 78. He used the file for approximately six months until 1995 and did not share the file with anyone. Tr. at 78. The Individual, during his disclosure to the SIO, raised the file's existence and inquired whether the file should be classified. Tr. at 79-81. The Individual believed, at the time the file was created, that the file did not meet the guidelines for classification. Tr. at 80. The SIO, after inquiring about the file, asked the Individual to erase the file, which he did. Tr. at 80. To ensure this situation could not occur again, the Individual has made it his practice to ask for a "classifier" to review any document or file he has any question about. Tr. at 82-83. Further, he

[11] The Individual turned over all of the personal drives to the SIO for examination and destruction. Tr. at 58.

has increased his awareness of this issue and his attitude is now to assume that any document is classified unless he is sure that the document is unclassified. Tr. at 82-83.

With regard to the SCIF Thumb Drive Incidents, the Individual testified that upon further reflection, he believes that he only took the drives into the SCIF two times and not five as he admitted in the 2012 PSI.[12] Tr. at 84. The Individual believes that he informed the SIO that he had taken thumb drives into a SCIF only two times. Tr. at 83. On the occasions he took the drives into the SCIF, he was wearing a coat with about six pockets in it. Tr. at 87. After going into the SCIF, the Individual discovered that he had the thumb drives in his coat. Tr. at 87, 88. When he discovered that he had the thumb drives he immediately powered down the computer he was using in the SCIF and left. Tr. at 88-90. However, he did not report the incident to the SIO because he was embarrassed and afraid of the consequences. Tr. at 88. During neither incident did the Individual use his thumb drives on the classified system. Tr. at 90. He does not believe that this type of situation will occur again since he now wears a different coat with two pockets and he does not use personal thumb drives in his work. Tr. at 87, 91. Additionally, when he goes to a SCIF, he takes his coat off and empties his pockets. Tr. at 91. He adopted these steps pursuant to his root-cause analysis. Tr. at 91.

As for the Cell Phone Incident in 2009, the Individual testified that after he discovered that he had inadvertently taken a personal cell phone into a security area, he immediately contacted the SIO to report this incident. Tr. at 93. However, when the incident was repeated in 2010, he did not report the incident to SIO. Tr. at 93. In both cases, the Individual did not realize he had a cell phone in his possession when he entered the security areas. Tr. at 94. Both the 2009 and 2010 meetings were unclassified so the Individual made the decision not to immediately leave the security area upon discovery of the phone but to wait until the meetings ended. Tr. at 95. The Individual did not report the 2010 cell phone incident since he was "embarrassed and ashamed" and he was afraid that he would get a formal security infraction. Tr. at 97. The Individual now avoids this situation by deliberately searching himself before going into security areas. Tr. at 98. The Individual's current cell phone is much larger now so that it is less likely he could inadvertently take his cell phone into a security area. Tr. at 99. Additionally, the Individual has a new attitude regarding reporting security incidents – that the national security of the government is important in protecting the national defense. Tr. at 98.

The Individual testified that, in 2003, during the Data Incident, he was part of a team evaluating a facility. Tr. at 100. His role in this team was to take data that the team collected and enter it into the Individual's software program. Tr. at 101. The team was to use computer hardware provided by the facility. Tr. at 100. During the evaluation the team came together and provided the Individual with data to be put into the Individual's software. Tr. at 102. None of the Individual's fellow team members indicated that the data was classified. Tr. at 102. After putting in some of the data, the Individual stopped and decided that he would not enter any additional data because the form of the data was such that someone might be able to use the data to derive classified information and that there was no classified computer available for the team. Tr. at 103-05. During this process, the Individual felt "pressure" to enter data. Tr. at 102. To avoid a similar situation, the Individual would be more proactive in raising an issue regarding data entry

[12] In the 2012 PSI, the Individual stated that he might have taken such drives into an SCIF on two occasions but that it might have been as much as on five occasions. Ex. 9 at 67.

into an unclassified computer and ensuring that he obtains a classification guideline briefing before going on a future project. Tr. at 106. With this information, he believes that he is better able to resist pressure to perform an action he feels is incorrect. Tr. at 107.

After making all of his disclosures to the SIO, the Individual's organization required the Individual to present a "lessons learned" presentation – a presentation of findings from his organization's root-cause analysis of why the security errors occurred.[13] Tr. at 30-31. In preparing the presentation, the Individual worked with an official at the SIO and his supervisor. Tr. at 32. The Individual presented his lessons-learned presentation in August 2011 to his immediate work group of 20-30 co-workers. Tr. at 33. In his presentation, the Individual stressed that his failure to report had been caused by his own fear that his career would be over and that reporting security incidents does not mean that one's career would be ended. Further, the Individual emphasized that the earlier you report potential security incidents, the more likely that the SIO would apply mitigating factors regarding the incident. Tr. at 34. While the Individual felt shame in having to make the presentation regarding his lapses to his co-workers he is glad he did so in that he has regained a sense of integrity. Tr. at 34. The Individual no longer views reporting incidents to the SIO as a punitive process. [14] Tr. at 111.

As to his failure to report these incidents earlier, the Individual testified that he had a deep sense of embarrassment and shame over the incidents since the Individual had been a physical security professional for over 25 years. Tr. at 27-28, 44-45. However, after having time to reflect upon these various security incidents, as a result of the root-cause analysis and creating his presentation, he now knows that his embarrassment is less important than the duty to report. Tr. at 110. Further the Individual believes, as a result of his disclosures and his mindset, that he cannot now be compromised. Tr. at 112-13.

B. The Team Lead's Testimony

The SIO Team Lead testified that she became familiar with the Individual when he came to the SIO to discuss past incidents that may have caused his polygraph to produce an inconclusive result.[15] Tr. at 171. The Team Lead was not involved in the initial discussions with the Individual concerning the possible security issues but worked with the Individual regarding the root-cause analysis of his security lapses and the lessons learned presentation that would be made from this analysis. Tr. at 174. The Team Lead testified that the Individual went beyond the effort

[13] The Individual was on the team from his organization that conducted the root-cause analysis. Tr. at 188.

[14] The Individual testified that his tendency to magnify the damage to his career that would result from disclosing security issues may have been aggravated by a psychological condition for which he is currently seeking treatment. Tr. at 151; Ex. C (counseling records). The Individual's condition was not cited as a security concern.

[15] The SIO Team Lead testified that individuals do not "fail" polygraph examinations. Instead, polygraph results may be deemed to be "inconclusive." Tr. at 173. If an individual produces an inconclusive result, another group at the facility will talk to that person to inquire further about any inconclusive results. If the ensuing discussion entails a possible security issue, the person is referred to the SIO for follow up. Tr. at 173. In the present case, the Individual initiated contact with the SIO. Tr. at 173-74.

that others had made in preparing similar presentations.[16] Tr. at 175. Significantly, the Individual asked the SIO to provide comments on his presentation. Tr. at 175. The SIO is not typically asked to review these types of presentations. Tr. at 175. The purpose of the root-cause analysis and the lessons learned presentation is to ensure security issues don't happen again. Tr. at 188. While the Team Lead believes the Individual will not commit similar security lapses in the future, the lessons learned presentation seeks to educate other employees to do the correct actions even if they have feelings similar to that of the Individual. Tr. at 188.

The Team Lead believes that the Individual was thoughtful in preparing the lessons learned presentation involving introspection and reflection of his errors. Tr. at 176. As evidence of this, the Team Lead cited the Individual's openness to add material to his presentation to ensure that the message on how to avoid making these security errors and to encourage others not to be afraid to contact the SIO when these issues arise. Tr. at 176-77.

With regard to the Individual's fear of reporting his errors to the SIO, the Team Lead testified that when she began to work at SIO approximately five years ago, some of the SIO personnel came from backgrounds such that they used "command voice" and "command presence" in dealing with employees reporting to the SIO. Tr. at 178. Consequently, this type of behavior would discourage employees from reporting. Tr. at 178. The SIO has worked for the past two and one-half years to change that perception and to send the message to employees that reporting incidents is "okay" and that it would not result in a loss of a job or clearance. Tr. at 178-79. As a result the SIO's call volume has doubled. Tr. at 179. Nevertheless, more tenured employees, such as the Individual, have a perception of the SIO as punitive and intimidating. Tr. at 180. As a result of the Individual's interaction with the SIO, the Individual no longer has those negative views of the SIO. Tr. at 180. The Individual is now a frequent caller to SIO with questions regarding security issues and shows no signs of embarrassment or fear. Tr. at 180.

The Team Lead further testified that a "Security Infraction" is a determination by the SIO following an inquiry as to who is responsible for a security incident but is not a disciplinary action. Tr. at 183-84. The SIO assigned security infractions based upon applying the facts of the incident to four criteria.[17] Tr. at 183; See Ex. 7 at 2. In the case of the Individual, he was assigned a security infraction for the sole reason of his delay in reporting the incidents to the SIO. Tr. at 182. Such security infractions are reported to an employee's supervisor for a determination whether disciplinary action against an employee is warranted. Tr. at 184.

C. The Former Supervisor's Testimony

The Individual's Supervisor testified that he has known the Individual for approximately 25 years and has worked closely with him as his supervisor on various occasions over the past five years. Tr. at 155-57. The Supervisor acknowledged the Individual's level of expertise of in a number of subject areas. Tr. at 156. In all the time the Supervisor worked with the Individual, he

[16] In this regard, the Individual testified that an employee's center coordinator will typically prepare the lessons learned presentation for the employee to present. Tr. at 175.

[17] The four criteria are: timeliness of disclosure; effect of incident on security interest; cooperation with security inquiry; and prior security incidents. Ex. 7 at 2.

never observed the Individual violate security rules or to be carless regarding such rules. Tr. at 160, 163. Further, the Former Supervisor observed that the Individual always was serious about security rules. Tr. at 160. Despite the Individual's admitted violations of security rules, the Supervisor believes that the Individual should retain a security clearance. Tr. at 160. Based upon working with the Individual and his observation of the Individual during the past 25 years, the Supervisor also believes that the Individual will avoid any future security violations. Tr. at 167. Additionally, the Supervisor confirmed the Team Leader's testimony regarding the attitudes of employees toward the SIO. Tr. at 160-63.

D. The Current Supervisor's Affidavit

In an affidavit, the Individual's current supervisor (Current Supervisor) attested that he would have testified on behalf of the Individual but he would be on official international travel on the date of the hearing. Ex. D. at 2. The Current Supervisor has known the Individual for 30 years and recognizes the Individual as an expert in his field. Ex. D at 1. The Current Supervisor was the Individual's supervisor at the time when the Individual made his "lessons-learned" presentation. Ex. D at 1. As part of the discipline to be imposed on the Individual, the Individual suggested that he make a "lessons-learned" presentation to their organization. Ex. D. at 1. He has spoken to the Individual for several hours concerning the incidents. Ex. D. at 1. During the Individual's presentation, the Individual presented the circumstances relating to the incidents, discussed why he had made the errors and provided advice to the audience on how to avoid similar security incidents. Ex. D. at 1. The primary emphasis of the Individual's presentation was that the employees should report security incidents immediately and that they should not be fearful to consult the SIO. Ex. D. at 1. Based upon his close observation of the Individual, the Current Supervisor believes that the Individual is honest, trustworthy, and reliable and has been diligent about non-classified security issues since his current difficulties. In the Current's Supervisor's opinion, the Individual has learned and grown from his experience surrounding the incidents that are the subject of the hearing. Ex. D at 2.

VI. ANAYLSIS

A. *Criterion G*

The Criterion G derogatory information centers on the Individual's failure to protect classified information or to comply with classified computer rules and regulations. The Individual does not dispute that the incidents occurred but believes that the Criterion G incidents were infrequent when compared to his 30-year career and that he has totally changed his mindset regarding the need to rigorously obey security rules and regulations. The Individual asserts that he now is dedicated to contact the SIO if an incident does occur.

As an initial matter, I found the testimony of the Individual and his witnesses to be believable and convincing. The witnesses' demeanor convinced me that each was sincere in their observations. I believe that the Individual, to the best of his ability, has tried to recollect every potential security incident in which he may have been involved.

As to the Criterion G allegation relating to the Individual's admission that he "failed" a polygraph test, I do not find that this admission is, in itself, a Criterion G concern. The Team Lead testified that the current practice with regard to the polygraph does not recognize someone failing a polygraph. More important, with regard to the question that produced inconclusive results which led to the Individual's recollection of the security incidents, as to whether he had ever provided information to foreign groups, there is no information in the record to indicate that the Individual provided information to such groups. Further, the SIO's analysis of the Individual's security errors indicated that there was little or no chance that classified information had been compromised. Tr. at 183.

My review of the Document Incidents indicates that the Individual made two inadvertent and isolated mistakes. I make this finding in light of the Individual's 30-year history of employment and his extensive experience in handling classified documents. Tr. at 81 (Individual testimony of having created hundreds of classified documents); Tr. at 160, 163 (Former Supervisor's testimony that he had never observed Individual violate security rules).

The Excel File Incident originated from the file's creation in 1994. Regardless as to whether the file should have been reviewed by a derivative classifier, the isolated nature of the event combined with the fact that this incident occurred some 19 years ago mitigates the Criterion G concern raised by this incident. To the extent that one can assume that this incident is recent because the Individual did not seek to have the file examined until recently, I find that the fact that the SIO asked the Individual to erase the file without further inquiry as to whether it was classified indicates the *de minimus* nature of this incident. Tr. at 79-80.

In reviewing the evidence regarding the Thumb Drive Incidents, the Individual has maintained that he was not aware of any prohibition regarding the use of personal data storage equipment when he used his personal thumb drives and hard drive to store non-classified work information. His lack of knowledge does not provide mitigation as to this incident since it is uncertain from the evidence whether the use of such devices was prohibited at the time he started to use them. At a minimum, it would appear that the Individual was negligent not to have sought advice whether such devises were allowed to be used for non-classified documents. However, it seems unlikely that the Individual will make a similar mistake again since he and other employees at the facility have been given the use of specially protected thumb drives to access and transfer such documents.

With regard to the Password Incident, I find little mitigation in the Individual's account of how this incident arose. Further, the incident is relatively recent. However, there is no evidence in the record indicating that the Individual has made similar errors over the course of his 30-year career. Further, I found the Individual's testimony convincing as his belief that the initial advice he received regarding how to store the password was incorrect and that his effort to store the password was an attempt to provide a more secure location to store the password. I found the Individual's testimony convincing regarding to his dedication not to repeat this error again by first contacting a computer security official. Importantly, I find the Individual's new mindset as to security as prompted by his root-cause analysis and lessons learned presentation will ensure that a similar occurrence will not occur in the future. *See infra*.

In the Individual's case, the most troubling Criterion G derogatory information is the Individual's failure to report incidents to the SIO. It is apparent that the Individual made a deliberate decision not to report the incidents because of shame, embarrassment, or his calculation as to how reporting such an incident might affect his career. Such an attitude presents a definite security risk. This is emphasized by the fact the Individual was assigned a security infraction primarily on his failure to report the Document Incident in a timely manner. However, as I alluded to above, I find that the Individual's testimony convincing as to the change of his attitude towards reporting security incidents and the need to be forthcoming resulting from the reflection and self-appraisal the Individual undertook as part of his root-cause analysis and his interaction with the SIO. Further the culture change described by the Team Lead with regard to reporting security incidents will encourage the Individual's compliance with reporting requirements. *See Personnel Security Hearing*, Case No. PSH-12-0083 (2012) (positive effect of similar culture change regarding security incident reporting on an individual). These conclusions are supported by the testimony of the Team Leader and the affidavit from the Individual's supervisor. The Team Leader has noted the Individual increased willingness to contact the SIO and his changed opinions regarding reporting incidents to the SIO. Further, in her testimony, the Team Lead opined that she believes that the Individual will not be involved in security incidents in the future. Tr. at 188. The affidavit affirms the Individual work in trying to analyze and incorporate changes in his attitude and conduct regarding security requirements. After reviewing all of the evidence and testimony, I find that the Individual's participation in the root-cause analysis, the lessons learned presentation and his work with the SIO concerning these programs have fundamentally changed the Individual's willingness to scrupulously conform to security regulations and report future security incidents. In sum, I find that the Individual has resolved the concerns raised by the Criterion G derogatory information described in the Notification Letter.

B. *Criterion L*[18]

Two of the events cited as Criterion L derogatory information, the SCIF Thumb Drive Incidents and the Cell Phone Incidents, I find are the result of unintentional, yet negligent, actions on behalf of the Individual. I am convinced by the Individual's testimony that he did not mean to bring the thumb drives or the cell phones into restricted areas and did not use the items while in the restricted areas. Further, the SIO concluded that the risk that his actions compromised any security measures was remote. The Individual no longer carries personal thumb drives to work and now institutes a personal practice to insure that he will not take prohibited items such as cell phones or other information technology equipment inside a SCIF. Consequently, I conclude that the Individual has mitigated the LSO's concerns regarding these two incidents.

With regard to the Hard Drive Incident, I note that the incident occurred almost five years ago. As with the Cell Phone and SCIF Thumb Drive Incidents, the SIO found that the Individual was unlikely to have compromised security with the use of the personal hard drive. Most significantly, as described above, I find that the Individual's changed mindset that resulted from his root-cause analysis, his lessons learned presentation, and his changed attitudes concerning consulting with the SIO make it very unlikely the Individual would try to use personal security hardware with his employer's computer systems.

[18] I will not separately discuss the Criterion G incidents also included as Criterion L incidents.

The Data Incident occurred almost 10 years ago. As such, the age of this incident and the unique circumstances under which it occurred provide mitigation. Given the fact that the Individual received pressure from his team members to enter the data indicates that the Individual should not shoulder full responsibility for the incident. Significantly, I find that the Individual did eventually stop entering data on his own. There is also some doubt as to whether the file, in fact, became classified when the additional data was entered. I believe that the Individual, because of his change in attitude regarding consulting with the SIO is better able to proactively seek help should such a situation occur in the future. I find that the Individual has resolved the concern raised by the Data Incident.

Even though I have determined that the Individual has mitigated each of the security concerns contained in the Notification Letter, the principal concern is nevertheless whether the Individual will act in the future in a manner that places the national security at risk by not rigorously following security procedures. 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. I find that the Individual's change in mindset in this regard began when he undertook a searching review of anything in his past that could have cause this result. In making this review he has tried to reveal everything in his memory, even events occurring long ago. The Individual has gone beyond the measures usually expected in resolving security incidents. The Individual is now a frequent user of SIO. The record convinces me that his vigilance regarding security concerns is now stronger than ever, especially in light of the humbling experience the Individual has undergone in the lessons learned presentation to his colleagues and the administrative review process. I also found the Team Leader's testimony regarding her assessment that the Individual is unlikely to have future security incidents to be persuasive. Consequently, I find that the Individual has mitigated concerns regarding his mishandling of classified material, and his honesty, reliability, and trustworthiness. *See Personnel Security Hearing*, Case No. PSH-12-0083 (2012) (similar security concerns mitigated).

VI. CONCLUSION

Upon consideration of the entire record in this case, I find that there was sufficient evidence to raise doubts regarding the Individual's eligibility for a security clearance under Criterion G and L of the Part 710 regulations. Further, I find that the Individual has presented sufficient evidence to resolve the concerns raised by the Criterion G and L derogatory information. Therefore, I conclude that restoring the Individual's 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). Accordingly, I find that the DOE should restore the Individual's 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.

Richard A. Cronin, Jr.
Hearing Officer
Office of Hearings and Appeals

Date