February 12, 2009

DEPARTMENT OF ENERGY
OFFICE OF HEARINGS AND APPEALS

Initial Agency Decision

Name of Petitioner: Dean P. Dennis

Date of Filing: August 14, 2008

Case Number: TBH-0072

This Initial Agency Decision concerns a whistleblower complaint (the "Complaint") filed by Dean P. Dennis (Mr. Dennis or the "Complainant") against his former employer, National Security Technologies, LLC (hereinafter referred to as "NSTec"), under the Department of Energy's (DOE) Contractor Employee Protection Program regulations set forth at 10 C.F.R. Part 708. At all times relevant to this proceeding, NSTec managed and operated the Nevada Test Site and other satellite facilities for the DOE's National Nuclear Security Administration's (NNSA) [1] Nevada Site Office. Mr. Dennis alleges in his Complaint that during his employment tenure with NSTec he made several disclosures protected under 10 C.F.R. Part 708 and that NSTec terminated him in retaliation for his having made those protected disclosures. Mr. Dennis seeks monetary damages, reimbursement of medical bills for a one-year period beginning from the date of his termination, an offer of re-employment with NSTec, an apology letter, a letter of recommendation, the deletion from his personnel and personnel security files of any reference to his "termination for cause" and a notation in his personnel and personnel security files of "layoff" to explain his absence from the workplace after June 6, 2007. As discussed below, I have determined that the Complainant is not entitled to relief under 10 C.F.R. Part 708.

I. Background

A. The DOE's Contractor Employee Protection Program

The DOE's Contractor Employee Protection Program was established to "safeguard public and employee health and safety; ensur[e] compliance with applicable laws, rules, and regulations; and prevent[] fraud, mismanagement, waste and abuse" at DOE's government-owned, contractor-operated facilities. 57 Fed. Reg. 7533 (March 3, 1992).[2] Its primary purpose is to encourage contractor employees to disclose information which

[1] NNSA is a semi-autonomous agency within the DOE which Congress established in 2000.

[2] The DOE has amended the Part 708 regulations a few times since its original promulgation of the regulations. *See* 64 Fed. Reg. 12,862 (March 15, 1999) (interim final rule), amended, 64 Fed. Reg. 37,396 (1999), amended and finalized, 65 Fed. Reg 6314 (2000), 65 Fed. Reg. 9201 (2000) (technical correction).

they believe exhibits unsafe, illegal, fraudulent, or wasteful practices and to protect those "whistleblowers" from consequential reprisals by their employers. 10 C.F.R. Part 708. Under the Part 708 regulations, protected conduct includes:

> (a) Disclosing to a DOE official, a member of Congress, any other government official who has responsibility for the oversight of the conduct of operations at a DOE site, [the employee's] employer, or any higher tier contractor; information that [the employee] reasonably believes reveals-
>
> (1) A substantial violation of a law, rule, or regulation;
> (2) A substantial and specific danger to employees or to public health or safety; or
> (3) Fraud, gross mismanagement, gross waste of funds, or abuse of authority; or
>
> (b) Participating in a Congressional proceeding or an administrative proceeding conducted under this regulation; or
>
> (c) Subject to § 708.7 of this subpart, refusing to participate in an activity, policy, or practice if [the employee] believe[s] participation would –
>
> (1) Constitute a violation of a federal health or safety law; or
> (2) Cause you to have a reasonable fear of serious injury to yourself, other employees, or members of the public.

The Part 708 regulations set forth the process for considering complaints of retaliation filed pursuant to those regulations. The DOE's Office of Hearings and Appeals (OHA) is responsible for investigating Part 708 complaints, convening evidentiary hearings, issuing Initial Agency Decisions, and considering appeals. *See* 10 C.F.R. §§ 708.21-708.34.

B. Procedural Background

On August 10, 2007, Mr. Dennis filed a Part 708 Complaint against NSTec with the local DOE Employee Concerns Program (ECP) Office. After efforts to engage in mediation proved unsuccessful, the ECP Office transferred the Complaint in October 2007 to OHA for an investigation, followed by an administrative hearing. The OHA investigation was delayed for several months due to the potentially classified nature of Mr. Dennis' Part 708 concerns, and the resulting need to make arrangements to allow the OHA investigator to conduct interviews and store documents in a secure environment. On August 14, 2008, the OHA Investigator issued his Report of Investigation (ROI) in this case, and I was appointed the Hearing Officer in the matter on August 19, 2008.

On October 21 and 22, 2008, I convened an unclassified hearing on Mr. Dennis' Complaint and heard testimony from eight witnesses. Counsel for Mr. Dennis submitted seven documents into the record which he labeled as Exhibits A through G; Counsel for

NSTec tendered four documents which he designated as Exhibits 1 through 4. These exhibits will be referred to in this Decision as "Ex." followed by the appropriate numeric or alphabetic designation. The hearing transcript in this case will be referred to as "Tr."

C. Mr. Dennis' Part 708 Complaint

Under the Part 708 regulations, a complaint must specifically describe the disclosures that the complainant believes gave rise to the alleged retaliation. 10 C.F.R. § 708.12 (a)(2). In his Complaint, Mr. Dennis stated that he was terminated for "informing my management that I needed to disclose security problems" at the RSL. Complaint at 1. Mr. Dennis related that the details of his security concerns were classified and for this reason he did not articulate them in his Complaint. *Id.* In his Complaint, Mr. Dennis generally described his protected disclosures as revealing "gross mismanagement relating to security practices and major security vulnerabilities in a facility and relating to classified computer security within the DOE in general." *Id.*

In the ROI, the OHA investigator stated that Mr. Dennis' failure to specifically describe his disclosures in his Part 708 Complaint would ordinarily result in his Part 708 action being dismissed. *See* ROI at 4. The OHA investigator found, however, that it was reasonable and necessary for Mr. Dennis to withhold the specifics of his disclosures until he could convey them to an investigator in a secure setting because the substance of the disclosures could potentially be classified. *Id.* Accordingly, Mr. Dennis was permitted to correct the procedural deficiencies in his Complaint when he met face-to-face with an OHA investigator who held a security clearance.

After meeting with Mr. Dennis, the OHA Investigator identified six possible protected disclosures, four related to security matters and two related to management issues. *Id.* at 4-5. Specifically, those disclosures in the former category include: (1) alleged ineffective security procedures related to ACREM, (2) alleged inefficiencies and security problems related to security logs, (3) the alleged presence of tracker software of unknown origin on a classified computer, and (4) alleged inadequate security procedures for escorting workers performing construction repairs in the Sensitive Compartmented Information Facility (SCIF). As for those disclosures in the latter category, they pertained to: (1) NSTec's alleged failure to provide Mr. Dennis with software so he could efficiently and effectively conduct reviews of security logs, and (2) NSTec's change in the access rules for the SCIF and the alleged negative impact that change had on Mr. Dennis's productivity.

The OHA Investigator concluded based on the evidence gathered during his investigation that, with the exception of the alleged "tracker software" issue, Mr. Dennis could not reasonably have believed that any of the other five alleged protected disclosures revealed "a substantial and specific danger to public health and safety." *See* ROI at 11.

At the hearing, I allowed Mr. Dennis to provide documentary and testimonial evidence on all six alleged disclosures. In this Decision, I have reviewed all of Mr. Dennis' disclosures not only to determine if any of them can be characterized as revealing "a

substantial and specific danger to public health and safety," but also to determine whether any of the disclosures revealed a "substantial violation of a law, rule or regulation," or "fraud, gross mismanagement, gross waste of funds, or abuse of authority."

II. The Legal Standard

As noted above, the regulations set forth at 10 C.F.R. Part 708 provide an administrative mechanism for resolving whistleblower complaints filed by employees of DOE contractors. The regulations specifically describe the respective burdens imposed on the Complainant and the contractor with regard to their respective allegations and defenses, and prescribe the criteria for reviewing and analyzing the allegations and defenses advanced.

A. The Complainant's Burden

It is the burden of the Complainant under Part 708 to establish, by a preponderance of the evidence, that he or she made a protected disclosure, participated in a proceeding, or refused to participate as described in 10 C.F.R. 708.5, and that such act was a contributing factor to a retaliatory action. 10 C.F.R. § 708.29. The term "preponderance of the evidence" means proof sufficient to persuade the finder of fact that a proposition is more likely true than not when weighed against the evidence opposed to it. *See Joshua, Lucero*, Case No. TBH-0039 (2007),[3] *citing Hopkins v. Price Waterhouse*, 737 F. Supp. 1202, 1206 (D.D.C. 1990). In the present case, Mr. Dennis must make two showings in connection with his Part 708 Complaint. First, he must show that he disclosed information to NSTec management that he "reasonably" believed revealed, either "a **substantial** violation of law, rule or regulation," "a **substantial** and specific danger to employees or to public health and safety" or "fraud, **gross** mismanagement, gross waste of funds, or abuse of authority (emphasis added)." 10 C.F.R. § 708.5. If Mr. Dennis meets this threshold showing with regard to any of his alleged protected disclosures, he must next prove that at least one of his disclosures was a contributing factor to his termination. One way a complainant can meet this evidentiary burden is to provide evidence that "the official taking the action has actual or constructive knowledge of the disclosure and acted within such a period of time that a reasonable person cold conclude that the disclosure was a factor in a personnel action." *See David Moses*, Case No. TBH-0066 (2008), *Ronald Sorri*, Case No. LWA-0001 (1993).

B. The Contractor's Burden

If the Complainant satisfies his evidentiary burden, the burden then shifts to the Contractor to show, by clear and convincing evidence, that it would have taken the same action absent any protected disclosures. "Clear and convincing evidence" requires a degree of persuasion higher than preponderance of the evidence, but less than "beyond a reasonable doubt." *See Casey von Bargen*, Case No. TBH-0034 (2007). OHA Hearing

[3] 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 entered the case number of the decision in the search engine located at http://www.oha.doe.gov/search.htm.

Officers have recently relied on the Federal Circuit for guidance in evaluating whether the contractor has met its evidentiary burden in a Part 708 case. *See David Moses*, Case No. TBH-0066 (2008), *Dennis Patterson*, Case No. TBH-0047 (2008). Specifically, the Federal Circuit, in cases interpreting the federal Whistleblower Protection Act (WPA), upon which Part 708 is modeled, examines: (1) the strength of the [employer's] reason for the personnel action excluding the whistleblowing, (2) the strength of any motive to retaliate for the whistleblowing, and (3) any evidence of similar action against similarly situated employees . . ." *See Kalil v. Dep't of Agriculture*, 479 F.3d 821, 824 (Fed. Cir. 2007).

III. Findings of Fact

Mr. Dennis holds a Bachelor's degree in finance and an MBA degree in management. Tr. at 25. He has worked for a number of DOE contractors at different locations since 1990. *See* Complaint at 1, Ex. 1. For most of his employment history before joining NSTec, he had little, if any, experience working in matters relating to security or intelligence activities. Mr. Dennis worked at the Nevada Site Office beginning in September 2003 as an employee of another contractor. Ex. 1. The record reflects that sometime in the fall of 2006, the contractor that preceded NSTec at the Nevada Site Office reorganized. Tr. at 27, 278, 374. The position occupied by Mr. Dennis at the predecessor contractor was abolished and that contractor placed him in a position so he could stay employed. *Id.* at 374, Ex. 1. Mr. Dennis' position after the reorganization was that of a Senior Operations Specialist working in the Special Programs Department at the Remote Sensing Laboratory (RSL) located on Nellis Air Force Base. *See* Complaint at 1. On March 21, 2006, the Field Intelligence Element (FIE) Director at the RSL asked Mr. Dennis to assume additional duties as an Information Systems Security Officer (ISSO) at the Sensitive Compartmented Information Facilities (SCIF)[4] at the RSL and the Nevada Intelligence Center. *See* Ex. D. Mr. Dennis testified that he had no background or training for either Senior Operations Specialist position or the ISSO position. Tr. at 28, 56.

NSTec became the management and operating (M&O) contractor for the NNSA's Nevada Test Site and the Nevada Site Office on July 1, 2006. *Id.* at 40, 46. NSTec elected to maintain the organizational structure established by the previous contractor at the site, a structure which included the position encumbered by Mr. Dennis. Tr. at 28. The previous contractor's FIE Director also assumed the same job responsibilities and title with NSTec that he held with the previous contractor. According to the record, NSTec management recognized that Mr. Dennis had no background in the positions that he occupied but nonetheless believed that he was qualified for his positions with "some on-the-job training."[5] *Id.* at 375.

---

[4] A SCIF is an "accredited area, room, group of rooms, or installation where Sensitive Compartmented Information Facility may be stored, used, discussed, and/or electronically processed." *See* DOE Order 5639.8A at http://www.directives.doe.gov.

[5] Between March 2006 and his termination in June 2007, Mr. Dennis completed seven training courses, some of them multi-day, which covered cyber security and other security-related topics. See Ex. C.

During his tenure with NSTec, Mr. Dennis' responsibilities included completing System Security Plans for computer systems at the RSL and another location;[6] serving as one of two custodians for Accountable Classified Removable Electronic Media (ACREM) in the RSL;[7] reviewing print-outs showing activity for computer terminals for access denials or some sort of irregularity (hereinafter referred to as "security logs") at the RSL and another location; and performing Derivative Classifier (DC) functions for NSTec. *See* Performance Review at Ex. 1, Tr. at 57, 62, 104-105, 356-357.

NSTec operated as a "matrix" organization, meaning that employees supported the activities of, and reported to, a number of different supervisors and managers at the facility. Tr. at 118. As a result, Mr. Dennis' actions were subject to the scrutiny of several NSTec officials. Mr. Dennis' supervisor of record was Ron Gross, the Manager of Special Programs. Tr. at 275. Mr. Dennis' supervisor for technical matters relating to information security was Jeff Harvey, the Information Systems Security Manager (ISSM). *Id.* at 93. Mr. Dennis' supervisor for the functions that he performed in the SCIF at the RSL, was Loretta DeVault, the Deputy FIE Director and Special Security Officer. *Id.* at 226-227. When Ms. DeVault was absent, her assistant, Rhonda Fulkerson, a Security Specialist and Alternate Special Security Officer, acted in her stead. *Id*. at 328. All of Mr. Dennis' supervisors reported to Alan Will, the Deputy Director of the RSL and the Director of FIE. *Id.* at 381. These reporting chains are important to determining whether Mr. Dennis raised any protected disclosures to a person in a position superior to his own at NSTec.

Sometime in the winter or spring of 2007, a number of events occurred that are relevant to understanding and appreciating some of the issues in this case. First, NSTec, at the direction of the DOE, implemented new procedures for handling ACREM in response to an incident that had occurred at another DOE facility. *Id* at 235. Next, NSTec, again at the direction of the DOE, decided to enhance the security at its site by reducing the number of persons who could access the SCIF without an escort. *Id.* at 257. Among those no longer allowed unrestricted access to the SCIFs as a result of the access changes were Mr. Dennis and his supervisor of record. *Id.* at 302. Third, NSTec decided to prohibit all thumb-drives, personal and company-owned, from the work site. *Id.* at 266, 289.

The record indicates that Mr. Dennis did not react well to the security enhancements noted immediately above. With respect to the ban of thumb drives, Mr. Dennis approached his supervisor of record four or five times and tried to convince him that he needed the company-owned thumb drive to do his job. *Id.* at 289. Mr. Dennis even raised the issue to the FIE Director in an attempt to "get his thumb drive" back, but to no avail. *Id*. at 267. As for the restricted access to the SCIF, one witness described Mr. Dennis as being "very unhappy, very aggravated" when he learned that he no longer had unrestricted access to the SCIF. *Id.* at 239-240. Another witness related she had

---

6 By his own report, this task required him to understand the requirements of a Director of Central Intelligence Directive, DCID 6/3. Ex. 1.

7 According to Mr. Dennis, all the ACREM resided outside the SCIF at RSL. Tr. at 71.

"multiple, extremely intense and somewhat confrontational conversations" with Mr. Dennis about the new access procedures at the SCIF. *Id.* at 331. Mr. Dennis expressed his view that the new access rules inhibited his ability to do his work and negatively impacted his productivity. *Id.* Mr. Dennis' supervisor of record responded to Mr. Dennis' concern by noting that "if you live in a classified world, you must adhere to the rules." *Id.* at 303. As for the DOE's new rules for handling ACREM, Mr. Dennis voiced his opinion numerous times to his superiors in April and May 2007 that the security improvements were pointless and ineffective. *Id.* at 194. To support his viewpoint, he speculated that someone with malicious intent could defeat the security procedures by surreptitiously copying ACREM after checking it out from the custodian. He also posited several scenarios where he, as a trusted insider and ACREM custodian, could maliciously circumvent the procedures without detection. *Id.* at 62-85.

Based on my observation of the demeanor of the witnesses at the hearing and my assessment of their credibility, it appears that Mr. Dennis' relationship with those in charge of the SCIF at the RSL was strained and that Mr. Dennis was less than cooperative in acceding to the legitimate work-related requests of those in charge of the SCIF. The Assistant Special Security Officer in the SCIF at the RSL testified that she had problems with Mr. Dennis bringing CDs into the SCIF to destroy. *Id*. at 335. She stated that "anything that comes into the SCIF needs to be approved by the Special Security Officer or the Assistant Special Security Officer." *Id.* at 336. According to the Assistant Special Security Officer, Mr. Dennis brought disks or CDs into the SCIF multiple times each week. *Id*. at 344. She opined that this kind of media did not need to be destroyed in a SCIF and that she approached Mr. Dennis every time he brought materials into the SCIF to destroy. *Id.* at 344-346. She related that Mr. Dennis did not take the disks to her upon entering the SCIF, that he was uncooperative in allowing her to look at the documentation, and that he told her she did not need to know what he was working on. *Id.* at 336-338. The Assistant Special Security Officer claimed, but Mr. Dennis vehemently denied, that she told him multiple times not to bring CDs or disks into the SCIF to destroy. *Id.* at 345, 360. The Special Security Officer testified that the Alternate Special Security Officer reported to her that Mr. Dennis was taking paperwork from the SCIF and had become irate when the Alternate Special Security Officer requested to see the paperwork. *Id*. at 263-264.

NSTec conducted performance evaluations of its workforce in March 2007. In anticipation of completing Mr. Dennis' performance evaluation, Mr. Dennis' supervisor of record inquired about Mr. Dennis' performance and conduct of those with whom he regularly worked. Mr. Dennis' supervisor of record learned for the first time that several persons, including those in charge of the SCIF at the RSL, claimed to have had difficulty finding Mr. Dennis during the work day. *Id.* at 280, 282. In March 2007, Mr. Dennis' supervisor rated Mr. Dennis' performance as "satisfactory" based principally on the comments that he had received about Mr. Dennis' unavailability. *See* Ex. 1. Mr. Dennis objected strenuously to the rating and eventually elevated the matter to the FIE Director. The FIE Director refused to alter Mr. Dennis' performance rating. Tr. at 287.

At some point shortly after completing Mr. Dennis' performance review in March 2007, Mr. Dennis' supervisor of record reviewed some reports relating to the classification activities at the site. *Id.* at 291. At that point, the supervisor of record discovered that Mr. Dennis had derivatively classified "a lot" of documents. *Id.* This fact troubled the supervisor of record because Mr. Dennis allegedly lacked the technical expertise to review many documents. *Id.* at 291-293. The supervisor of record explained at the hearing that he was concerned that Mr. Dennis might have been privy to information that he should not have been due to the extensive nature of his derivative classification activities. *Id.* at 291. The supervisor of record immediately instructed Mr. Dennis to stop derivatively classifying documents unless Mr. Dennis was the only person available to perform that function and the document needed to get out. *Id.* at 292.

Sometime in late March 2007 or early April 2007, Mr. Dennis' supervisor of record and the Special Security Officer of the SCIF at the RSL independently met with the FIE Director to discuss their respective security concerns about Mr. Dennis. Mr. Dennis supervisor of record first expressed his concern to the FIE Director about Mr. Dennis' repeated requests to get his company-owned thumb drive back. *Id.* at 290. According to the supervisor of record, there was no reason why Mr. Dennis required a thumb drive to do his work. *Id.* The supervisor of record also shared with the FIE Director his concern about the excessive number of derivative classification reviews that Mr. Dennis had performed in light of the fact that Mr. Dennis might have lacked the technical expertise to review or even see some of the documents that he had derivatively classified. *Id.* at 291-293. Next, the supervisor of record advised the FIE Director that several persons had reported that Mr. Dennis was not available during the workdays. *Id.* at 291. In addition, the supervisor of record mentioned to the FIE Director that Mr. Dennis often worked times beyond normal work hours, including weekends. [8]*Id.* at 297. There were times, according to the supervisor of record, where Mr. Dennis would be isolated in his area even when there was a second person present in the facility.[9] *Id.*

The Special Security Officer of the SCIF at the RSL also reported numerous concerns about Mr. Dennis' behavior to the FIE Director. First, she told him that Mr. Dennis was aggravated with the security procedures that the DOE had put in place in the facility and had repeatedly expressed his view that the security procedures were ineffective. *Id.* at 239. Second, she related that Mr. Dennis had told her he could do "damage and walk away with things." *Id.* Third, she stated that Mr. Dennis was under a lot of emotional and financial stress due to his divorce and contested child custody issues. *Id.* Fourth, she advised the FIE Director that Mr. Dennis had become very upset with NSTec's prohibition of thumb drives in the work place. *Id.* Fifth, she related that Mr. Dennis had expressed concerns about passing a polygraph examination because he needed to

---

[8] The supervisor of record testified that NSTec had sanctioned some of Mr. Dennis' unusual work hours in an effort to accommodate his childcare issues. *Id.* at 298.

[9] The supervisor of record testified that there was a two-person rule in the building where Mr. Dennis worked, meaning that there needed to be two persons present at the location at all times for purposes of security and accountability. *Id.*

manipulate an insurance claim in order to be made whole after a serious automobile accident. *Id.* at 264-265.

In addition to the litany of concerns enumerated above by Mr. Dennis' supervisor of record and the Special Security Officer, the FIE Director testified that the Special Security Officer had also raised a concern that Mr. Dennis had been visiting sites on the classified network where he should not have been going. [10] According to the FIE Director, he communicated all the concerns that he received about Mr. Dennis in early April 2007 to his senior management at NSTec and to the DOE organization responsible for overseeing NSTec's operations. *Id.* at 384.

In mid-May 2007, Mr. Dennis reported to the ISSM that there was tracking software on his computer. *Id.* at 96. The ISSM immediately brought this matter to the attention of the Special Security Officer. [11]*Id.* at 418. The FIE Director testified that the ISSM also informed him of Mr. Dennis' computer software tracking discovery. *Id*. at 402.

While the DOE was reviewing the allegations relating to Mr. Dennis that NSTec had brought to the agency's attention in early April 2007, Mr. Dennis sent an e-mail to the FIE Director on May 31, 2007, in which he related his accomplishments for the week and asked to discuss the negative impact the new SCIF access requirements were having on his ability to do his job. *See* Ex. 3. On June 1, 2007, Mr. Dennis sent another e-mail to the FIE Director, this one elaborating on the impact his restricted SCIF access was having on his work. *See* Ex. 2. A meeting to discuss Mr. Dennis' SCIF-related concerns was scheduled in the FIE Director's office for June 6, 2007. *See* Complaint at 1.

At some point, the DOE allegedly decided that the agency could no longer support Mr. Dennis working in the SCIF environment in view of the information NSTec had presented to the agency and its own analysis of the situation. *Id.* at 388. The FIE Director testified that the DOE advised NSTec that it was NSTec management's decision whether to find another position for Mr. Dennis. *Id*.

Sometime in early June 2007, several high level NSTec managers, including the company President met to discuss Mr. Dennis' future with NSTec. *Id.* at 447. The NSTec President testified that those assembled unanimously agreed to terminate Mr. Dennis' employ. *Id.* at 448. According to the NSTec President, Mr. Dennis had exhibited an aggressive pursuit of highly classified information that was deemed not relevant to his job assignment. *Id.* Mr. Dennis' persistent demands to access classified information and his financial situation were alleged to be among the reasons for his termination. *Id.* at 450.

---

[10] It appears from the record that Mr. Dennis did access classified sites that he should not have. Under cross-examination, Mr. Dennis claimed that he had the right to access [certain sites] even if he didn't have a "need to know" because he thought he was being groomed for a position in intelligence. *Id.* at 187-188.

[11] There is some conflicting testimony on this matter. The Special Security Officer claims to have no recollection of the ISSM raising the issue of tracking software with her. *Id.* at 244. Instead, her recollection is that the ISSM communicated to her that Mr. Dennis' administrative rights to the computer had been taken away from him. *Id.* at 247. Based on my assessment of the demeanor and credibility of the witnesses, I find that the ISSM did report Mr. Dennis' belief to the Special Security Officer.

After the NSTec management decided Mr. Dennis' fate, the Employee Relations Manager for NSTec prepared the necessary paperwork and Mr. Dennis was terminated on June 6, 2007. *Id.* at 476. Ex. 1.

IV. Analysis

A. Whether the Complainant Made any Disclosures Protected under 10 C.F.R. Part 708?

As noted in Section I.C. above, Mr. Dennis alleges that he made six protected disclosures during his tenure with NSTec. Two of those disclosures involve the same subject matter, *i.e.*, security logs. For purposes of this Decision, the alleged disclosures relating to security logs will be analyzed together.

1. Allegations regarding ineffective security procedures relating to ACREM

It is undisputed that, in April and May 2007, Mr. Dennis expressed his view to the Special Security Officer whose responsibility it was to oversee the SCIF at the RSL that the new procedures imposed by the DOE on the handling of ACREM were ineffective. Tr. at 234-236. To support his opinion on this matter, Mr. Dennis suggested that someone could bring a thumb drive or a disk into the facility and improperly download materials. *Id.* at 72. Mr. Dennis also suggested at the hearing that he could take a disk from the facility, go into his vehicle, copy the disk onto a laptop, and then return the disk to the facility without detection. At the hearing, Mr. Dennis admitted that there are some security safeguards (i.e. strap seals over the ports) that might make it difficult for someone to copy ACREM. *Id.* at 73-74. However, he pointed out that as the ACREM custodian, he was "in control of all the strap seals" and if he "were a bad guy" he could compromise security. *Id.* In fact, on several occasions, Mr. Dennis expressed his opinion to the Special Security Officer that he, as a custodian of ACREM, had too much authority and could pose an "insider threat" to NSTec. He also detailed some hypothetical fact scenarios where he could do damage to the facility. *Id.* at 68-85. Finally, at the hearing, Mr. Dennis raised for the first time his claim that the configuration of the software being used to comply with DOE's new ACREM requirements was deficient and that he had been prevented from elevating his concerns in this regard to senior management at NSTec.

As an initial matter, I find that Mr. Dennis' allegations relating to ACREM are all based on speculation. He admitted at the hearing that his concerns were grounded in what "potentially" could happen and that he never observed anyone do anything remotely approximating the security breach scenarios that he posited. *Id.* at 79. I also inferred from his testimony that he had never knowingly engaged in any conduct that had potentially compromised the security of the systems that he oversaw. Moreover, the record is clear that NSTec had banned the use of all thumb drives, including company-owned thumb drives, at its facility to enhance its security posture. I find it curious then that Mr. Dennis

raised the issue of thumb drives in connection with ACREM as a potential security concern when it was he who vociferously objected to this security enhancement when NSTec took his thumb drive away. With regard to Mr. Dennis' claim that he could have exited the facility with classified information and surreptitiously copied it onto a laptop in his car, he admitted under questioning by me that all vehicles entering and exiting the facility were subject to random search.[12] I was not convinced from Mr. Dennis' testimony that the physical security at the NSTec complex was non-existent, as he claimed. Regarding his contention that there were deficiencies in the configuration of the software used to prevent cyber security breaches, I was not convinced that Mr. Dennis possessed the technical expertise to render such an opinion. At the hearing, I asked Mr. Dennis how he knew enough about computers to do his job in view of his lack of background in the area. *Id.* at 56. He responded, "I didn't. That was the issue. . . I had no technical knowledge at all." *Id.* For this reason, I am unable to find that Mr. Dennis' belief about the possible deficient configurations in the ACREM software was reasonable.

In the end, I find that Mr. Dennis has not provided a preponderance of evidence that his statements about the ACREM are covered by the Part 708 regulations. First, since NSTec was following the DOE instructions on implementing the new ACREM procedures and Mr. Dennis did not allege that NSTec was not complying with DOE's mandate, neither a charge of gross mismanagement[13] nor a violation of a regulation or rule[14]could reasonably be argued here. Second, I find that Mr. Dennis could not reasonably have believed that NSTec's implementation of the ACREM amounted to a substantial and specific danger to employees or to public health and safety. It appears from the record that there were checks and balances in place in the locations where Mr. Dennis was handling ACREM. For example, the conflict between him and the Assistant Special Security Officer revolved around his introduction and destruction of ACREM in the SCIF at RSL. Mr. Dennis appears to have resented the intrusion of the Assistant Special Security Officer into his activities relating to ACREM when he was in a facility which she managed in an alternate capacity. She questioned him constantly, and asked to see

---

[12] The location where I conducted the two-day hearing in this case is one of the locations where Mr. Dennis spent a portion of his time while he was employed by NSTec. I personally observed security measures, including the random searches of vehicles entering and exiting the facility. It strains credulity, therefore, how Mr. Dennis could believe that there were no physical security measures in place at the NSTec facility.

[13] At the hearing, Mr. Dennis claimed that NSTec was "mismanaging how it handled ACREM." *Id.* at 79-80, 129-130. When questioned whether the mismanagement rose to the level of "gross" mismanagement, Mr. Dennis stated that NSTec's handling of ACREM did not constitute "gross mismanagement" but rather violated some rule, regulation, etc. *Id.* at 131. Later in his testimony, Mr. Dennis claimed that NSTec did engage in gross mismanagement because it did not do anything immediately about his ACREM concerns and prevented him from going to a higher level with the matter by firing him. *Id.* at 133-134.

14 In making this finding, I considered the testimony of the ISSM who characterized Mr. Dennis' "insider threat" comments as legitimate concerns expressed by one security professional to another. There was no testimonial or documentary evidence in the record to allow me to conclude that Mr. Dennis' concerns were anything more than rank speculation.

his paperwork for work being done in the SCIF. It was my impression from the Assistant Special Security Officer's testimony that the activities of those working at the NSTec facility were monitored by those with oversight responsibility. While it is possible that a trusted insider could breach security in any secure environment, it did not appear to me that there was anything fundamentally flawed with the new ACREM rules that would cause a reasonable person to believe that national security was at risk.

Finally, I find no evidence to support Mr. Dennis' claim that NSTec prevented him from advancing his concerns about ACREM up the chain of command. In fact, there was testimony in the record that the FIE Director had an "open door" policy and was generally available to NSTec employees. *Id.* at 376, 407. Mr. Dennis himself availed himself of the opportunity to speak to the FIE Director to complain about the thumb drives being removed and about issues relating to his performance evaluation. He could easily, it appears, had raised the ACREM matter directly with the FIE Director if he had chosen to do so.

2. Allegations regarding inefficiencies and security problems relating to security logs

Mr. Dennis was tasked with reconciling security logs which allegedly entailed his sifting through thousands of entries to identify anomalies. At the hearing, Mr. Dennis claimed that NSTec did not maintain its security logs in a "legal fashion." *Id.* at 105. In this regard, he stated that DCID 6/3 requires the separation of duties between administrators and the ISSO. *Id.* at 105. However, Mr. Dennis acknowledged at the hearing that such a separation did exist at the NSTec facility. *Id.* He also admitted at the hearing that DCID 6/3 did not require that software be put on computers for purposes of reviewing the security logs; it only mandated that the security logs be reviewed, not how to do it. *Id.* at 110. The evidence is clear that Mr. Dennis' disclosure about the security logs, if he articulated it to anyone,[15] did not reveal a substantial violation of a law, rule or regulation.

Mr. Dennis believed that the task of reviewing the security logs was cumbersome for him to perform. When Mr. Dennis learned that another DOE facility was using a software program to perform the function, he requested that NSTec purchase the software. *Id.* at 104, 129. At the hearing, Mr. Dennis admitted that NSTec never declined his request to purchase the software. *Id.* at 129. He also testified that he did not believe NSTec was engaging in gross mismanagement with regard to the requirements it imposed on him to review the security logs. *Id.*

Although the Assistant Special Security Officer denies it, Mr. Dennis claims that he told her that the security logs should be converted to a CD to prevent a system administrator from overwriting the entries. *Id.* at 103, 330. Mr. Dennis testified that "he was worried that someone might change the manual logs." *Id.* at 112. It appears from the evidence before me that Mr. Dennis was offering a "process improvement" to unburden him from

---

[15] None of the witnesses recall Mr. Dennis raising this issue with them.

the cumbersome task of manually reviewing the security logs. Mr. Dennis' unfounded speculation that someone might change a security log does not rise to the level of a reasonable belief protected under Part 708 that a security concern existed in the workplace with regard to the security logs.

3. Allegations about Tracking Software

Mr. Dennis alleges that in mid-May 2007, he reported to the ISSM that he had discovered an unauthorized software program on his classified computer in the SCIF. *Id.* at 96. Mr. Dennis testified that he noticed the presence of the software when he saw an unfamiliar icon in the lower right hand corner of his computer screen. *Id.* at 91. The ISSM confirmed at the hearing that Mr. Dennis showed[16] him the computer icon which appeared to be some sort of tracking software. *Id.* at 416-417. The ISSM testified that had grave concerns about this discovery, and immediately reported the matter first to the Special Security Officer in the SCIF[17] and then to the FIE Director. *Id.* at 418.

Mr. Dennis' supervisor of record testified that Mr. Dennis told him about the tracking software that he had discovered on his classified computer. *Id.* at 300. The supervisor asked him why the matter concerned him. *Id.* Mr. Dennis told the supervisor that he may have been "surfing on places where [he] shouldn't have been." *Id.* The supervisor responded by stating that he had no knowledge of any tracking software on the classified computers but if there was any tracking software, Mr. Dennis would need to answer for any of his unauthorized viewing of information on the classified network. *Id.*

The FIE Director confirmed at the hearing that the ISSM came to him with Mr. Dennis' concern about the tracking software. *Id.* at 378. The FIE Director provided probative testimony on the issue, the details of which need not be elaborated in this Decision, except that he was not concerned that any outsiders or "malicious folks" had hacked into NSTec's computer systems. *Id.* at 402-403.

Ultimately, it is not relevant whether the tracking software was installed with proper authorization, or even if tracking software was installed at all. Rather, I must look at whether it was reasonable for Mr. Dennis to believe that (1) unauthorized tracking software had been installed on the classified network in the SCIF, and (2) whether someone might have compromised the security procedures and rules at the SCIF by

---

[16] There is some conflicting testimony on this matter. Mr. Dennis claims that he called the ISSM into his office and asked him to look at the icon on his computer screen. *Id.* at 102. Mr. Dennis stated at the hearing that he did not print anything out. *Id.* The ISSM testified that Mr. Dennis "handed him a print of the name" of the software. *Id.* at 417. I need not resolve this conflicting testimony since I ultimately find that Mr. Dennis disclosed information to a supervisor, the ISSM, (either in person or by providing a print-out) that he reasonably believed revealed a substantial violation of security rules.

[17] The Special Security Officer claimed that she had no recollection of any conversation with either the ISSM or Mr. Dennis about Mr. Dennis' discovery of unauthorized tracking software on his classified computer. I did not find this testimony credible. Instead, I believed Mr. Dennis and the ISSM's account of their interaction with the Special Security Officer on this matter.

installing unauthorized software on the classified computer system. Mr. Dennis' testimony and that of the ISSM convince me that Mr. Dennis had a reasonable belief that there was unauthorized tracking software on his classified computer.[18] Specifically, Mr. Dennis' discovery of the icon on his computer and the ISSM's independent assessment of the situation clearly suggest that the two men reasonably believed that a cyber security breach may have occurred. In a classified setting, unauthorized tracking software, if it were truly unauthorized as Mr. Dennis believed, would clearly violate security rules, and potentially pose a significant threat to the national security. Mr. Dennis disclosed the presence of the tracking software to one of his superiors, the ISSM, and then to the Special Security Officer who oversaw the SCIF. In the end, I find that Mr. Dennis has proven, by a preponderance of evidence, that he made a protected disclosure regarding the tracking software on his classified computer.

4. Allegations of inadequate security procedures for escorting workmen in the SCIF

It is unclear from the evidence whether Mr. Dennis communicated his concern regarding the escorting procedures for construction workers in the SCIF to anyone. He testified that he did not speak to either the Special Security Officer or the Alternate Special Security Officer who oversaw the SCIF because they "seemed angry at [him] all the time." *Id.* at 141. He testified further that "he was going to" discuss the matter with the FIE Director, a statement that clearly indicates he had not done so. *Id.* at 140. He testified further that he told the ISSM, although the ISSM testified that he had no recollection of any such discussion. *Id.* at 414-415. Because Mr. Dennis could not prove that he disclosed this concern regarding the workmen in the SCIF to anyone, I find that he did not meet his evidentiary burden that he made a disclosure protected under Part 708 with regard to this discrete matter.

5. Allegations regarding changes to the SCIF access procedures

Mr. Dennis expressed his frustration with the new changes to the SCIF access procedures to the ISSM, the Assistant Special Security Officer, and his supervisor of record. *Id.* at 302, 331, 416. He also sent two e-mails to FIE Director requesting a meeting specifically to discuss the new access procedures. Ex. 2, 3.

The ISSM testified that Mr. Dennis did not consider the new access rules to constitute some sort of security breach. Tr. at 416. The ISSM explained to Mr. Dennis that he had no authority or oversight over the physical security at the SCIF, and directed him to share his concerns with the Special Security Officer at the SCIF or with the FIE Director. *Id.*

[18] Mr. Dennis' motive in revealing his discovery is not relevant here. Specifically, it is not relevant that Mr. Dennis may have been more concerned that the tracking software might uncover his possible misuse of the classified computer than with the potential security breach posed by that software. The DOE made it clear in the preamble to the 2000 amendments to the Part 708 regulations that it would not impose a "motives test" that could "allow an employee's intentions to be put on trial as a precondition to using the rule." See 65 Fed. Reg. 6314 (February 9, 2000).

The Assistant Special Security Officer at the SCIF related at the hearing that she had "multiple, extremely intense and somewhat confrontational conversations" about the SCIF access changes. *Id.* at 331. She stated that Mr. Dennis felt that the access changes inhibited his ability to do his work. *Id.*

The individual's supervisor of record testified that Mr. Dennis spoke to him about being excluded[19] from the SCIF. Id. at 302. The supervisor related that he, too, was excluded from the SCIF under the new rules. *Id.* He stated that he had no trouble under the new rules because he knew that NSTec was tightening its security by restricting access to the SCIF. *Id.*

At the hearing, Mr. Dennis testified that the SCIF access changes were inconvenient. *Id.* at 142. He related that he did not know the rules under which he was allowed to remain in the SCIF after he was escorted in there, and that the rules "kept changing." *Id.* at 214, 142. He clarified at the hearing that he did not consider his issues with the SCIF access changes to constitute gross mismanagement on the part of NSTec. *Id.* at 143. In addition, Mr. Dennis did not advance any argument at the hearing that would allow me to characterize his concerns about the new SCIF access procedures as a disclosure which revealed the substantial violation of some law, rule, or regulation, or a substantial danger to employee or the public health or safety. *Id.* Therefore, based on the evidence before me, I find that Mr. Dennis's concerns about the new SCIF access procedures do not fall within the ambit of 10 C.F.R. § 708.5.

6. Summary

In conclusion, for the reasons discussed above, I find that Mr. Dennis presented a preponderance of evidence that he made only one protected disclosure, a disclosure about the presence of tracking software on his classified computer. I turn next to whether Mr. Dennis has met the second prong of his evidentiary burden.

B. Whether Mr. Dennis' Protected Disclosure was a Contributing Factor in NSTec's Decision to Terminate Him?

In most cases, it is impossible for a complainant to find a "smoking gun" that proves an employer's retaliatory intent. Thus, Hearing Officers in Part 708 proceedings allow complainants to meet their burden of proof through circumstantial evidence. In prior cases, Hearing Officers have held that a protected disclosure may be a contributing factor in a personnel action where "the official taking the action has actual or constructive knowledge of the disclosure and acted within such a period of time that a reasonable person could conclude that the disclosure was a factor in a personnel action." *Ronald A. Sorri*, Case No. LWA-0001 (1993), *Thomas T. Tiller*, Case No. VWA-0018 (1997), *David L. Moses*, Case No. TBH-0066 (2008), *Richard L. Strausbaugh, et al*., Case Nos. TBH-0073, TBH-0075 (2008). In addition, "temporary proximity" between a protected

[19] Neither the Mr. Dennis nor his supervisor was "excluded" from the SCIF in the conventional meaning of that term. Rather, they both required an escort to enter the SCIF and their activities were monitored while in that location.

disclosure and an alleged act of reprisal is "sufficient as a matter of law to establish the final required element in a prima facie case for retaliatory discharge." *Ronald A. Sorri*, Case No. LWA-0001 (1993), citing, *County v. Dole*, 886 F.2d 147 (8th Cir.), *Janet Benson*, Case No. VWA-0044 (1999), *David L. Moses*, Case No. TBH-0066 (2008). Finally, a United States District Court has made it clear that a putative whistleblower must show both temporal proximity and knowledge to satisfy his or her regulatory burden. *See Safety & Ecology Corporation v. DOE*, Civil Action No. 03-0747 (D.D.C. 2004).

Applying these standards to the present case, I find that there is clearly temporal proximity between Mr. Dennis' protected disclosure in mid-May 2007 and his termination on June 6, 2007. I also find that at least one of those involved in the decision to terminate Mr. Dennis, namely the FIE Director, had actual knowledge of Mr. Dennis' protected disclosure. As previously stated in this Decision, the Field Intelligence Director testified that the ISSM told him in May 2007 about Mr. Dennis' concern about the computer tracking software. *Id.* at 378. The FIE Director also testified that he was one of seven senior NSTec managers who met in June 2007 and voted to terminate Mr. Dennis. *Id.* at 385-386. Accordingly, I find that Mr. Dennis has shown both temporal proximity and the knowledge necessary to meet his regulatory burden.

In sum, I find that Mr. Dennis has established a prima facie case that his protected disclosure was a contributing factor to his termination. The burden now shifts to NSTec to prove by clear and convincing evidence that it would have terminated Mr. Dennis absent his protected disclosure. 10 C.F.R. § 708.9(d).

C. Whether NSTec proved by clear and convincing evidence that it would have terminated Mr. Dennis even if he had not made a protected disclosure?

Under 10 C.F.R. § 708.29, NSTec bears a heavy burden in establishing that it would have terminated Mr. Dennis in the absence of his having made a protected disclosure. If NSTec meets this burden, however, it will defeat Mr. Dennis' allegation of retaliation in this case.

As an initial matter, I recognize that NSTec may have been prevented from providing as much testimonial evidence in support of its decision to terminate Mr. Dennis as it might have wished because I conducted the hearing in an unclassified format. In this regard, there were two occasions when NSTec witnesses (*e.g.* the FIE Director and the Special Security Officer) refrained from providing details for their responses because they were unable to do so in an unclassified forum.[20] *See* Tr. at 251, 388. Notwithstanding the constraints imposed on NSTec at the hearing, I find, as discussed below, that NSTec has

[20] A Classification Representative from DOE Headquarters accompanied me to the hearing. While I conducted the hearing in a secure location in an abundance of caution due to the potential classified overtones to the case, I admonished all witnesses that they were not to communicate any classified information to me during the hearing. On several occasions, I stopped the hearing at the request of a witness and permitted the witness to step outside the hearing room to speak with the Classification Representative to ensure that the witness' anticipated testimony would be unclassified.

provided clear and convincing evidence that it would have terminated Mr. Dennis even if he had not raised his concerns about the tracking software.

The testimonial evidence adduced at the hearing made it clear to me that once senior management at NSTec had "lost trust" in Mr. Dennis, they could no longer continue to assume the risk that Mr. Dennis might compromise national security while he occupied a position of major responsibility in a very secure environment. I was particularly struck by the testimony of NSTec's President whom I observed choose his words carefully and reflectively so as not to reveal classified information. The President, who remarked that he had held a top secret security clearance for several decades, expressed grave concern that Mr. Dennis had exhibited an "aggressive pursuit of highly classified information that NSTec deemed not relevant to his assigned job." *Id.* at 448. Explaining how "need to know" is the foundation of access to classified information, the NSTec President stated that Mr. Dennis' persistent demand to access classified information without the requisite "need to know" raised "a red flag of security concerns."[21] *Id.* at 449-450. The NSTec President testified that the decision to terminate Mr. Dennis was unanimous among those who assembled in June 2007 to discuss Mr. Dennis' behavior and conduct in the workplace. *Id.* at 448

Another senior manager who voted to terminate Mr. Dennis at a meeting convened in June 2007 also provided probative testimony at the hearing. The FIE Director first discussed the concerns brought to him by the Special Security Officer and Mr. Dennis' supervisor of record *(e.g.* Mr. Dennis' accessing of classified sites without a "need to know," his "insider threat" comments about himself, his unavailability, etc.) and then explained in detail how those concerns were elevated to the DOE. *Id.* at 381-385. The FIE Director also revealed that the DOE decided, after reviewing and analyzing the information presented to it by NSTec, that it would not support Mr. Dennis' activities in the SCIF. The FIE Director stated that DOE informed the company that it was free to find another position for Mr. Dennis in the company. *Id.* at 388. Finally, the FIE Director testified that NSTec was concerned about what Mr. Dennis could do as an insider, not what some hypothetical person could do to damage national security. *Id.* at 393.

Many of the concerns identified by both the FIE Director and NSTec's President as evidence of why the company "lost trust" in Mr. Dennis are corroborated by hearing testimony in the record. With regard to Mr. Dennis' persistent attempts to access classified information that he did not need to complete his job assignments, the following testimonial evidence is relevant. First, Mr. Dennis admitted on cross-examination that he thought it was permissible for him to access classified information even if he did not have a "need to know" because he thought he was being groomed for a position in the intelligence.[22] *Id.* at 187-188. I found this admission very disturbing for a former DOE

---

[21] The President also expressed a concern about Mr. Dennis' financial situation. However, NSTec did not provide any evidence of Mr. Dennis' financial irregularities. Had NSTec's only articulated reason for terminating Mr. Dennis been because of Mr. Dennis' financial situation, I would not have found any credible evidence to support that concern.

[22] When pressed at the hearing, Mr. Dennis acknowledged that he did not have "carte blanche" to access any classified site that he wanted. *Id.* at 187-188.

security clearance holder. The President of NSTec is correct that the "need to know" is the foundation for all activities involving classified information. Second, Mr. Dennis' supervisor of record testified convincingly of his concern in learning that Mr. Dennis had proactively sought out "a lot" of derivative classification assignments which might have given him access to classified material that he should not have had and for which he lacked the technical expertise. *Id.* at 291-296. Third, several managers expressed concern about Mr. Dennis' repeated vocal objections to the NSTec's decision to remove all thumb drives from the work site and his elevation of the matter to the FIE Director. *Id.* at 239, 289-290. As noted by Mr. Dennis' supervisor of record, Mr. Dennis' reaction to the enhanced security measure was perplexing given that he did not need a thumb drive to do his work. *Id.* at 290. Mr. Dennis' persistence in trying to get his company-owned thumb drive[23] returned raises a concern whether he had been downloading classified information and removing it from the work site, a scenario that he suggested on several occasions was possible in his work environment. Further, the Special Security Officer testified about Mr. Dennis' possible fraudulent manipulation of an insurance claim for pecuniary gain as a reason why he was concerned about undergoing a polygraph examination. The specter of possible fraudulent activity on Mr. Dennis' part is troubling in that it raises a question about his honesty, his willingness to comply with rules and regulations, and his potential violation of the law. The record already contains some evidence that Mr. Dennis might have been less than diligent in complying with security rules. Specifically, the Assistant Security Officer testified that Mr. Dennis was not always compliant with the SCIF requirement that, upon entering the SCIF, he provide the Special Security Officer with any material that he carried into the SCIF so she could examine it. *Id.* at 337. The Assistant Special Security Officer further testified those exiting the SCIF were subject to inspection to ensure that no classified material is removed from the SCIF. *Id.* According to the Assistant Special Security Officer, one time when she challenged Mr. Dennis, he reportedly told her that she did not need to know what he was working on. *Id.* at 338. She related that she continued to press the issue with Mr. Dennis which resulted in his leaving the document in the SCIF.

Turning to the factors set out in *Kalil v. Dep't of Agriculture*, 479 F.3d 821, 824 (Fed. Cir. 2007), I find that NSTec has provided strong evidence that Mr. Dennis' behavior in the workplace, most notably his aggressive pursuit of classified information without a "need to know," his seeming disregard of the rules in the SCIF, and his characterization of himself as an "insider threat," raised legitimate suspicions that he might be failing to properly safeguard classified information. This conduct must necessarily be evaluated in the context of very secure environment in which Mr. Dennis worked to appreciate fully why it potentially implicated national security. If one chooses to work in a classified environment, one must be trusted to adhere strictly to stringent rules and endure restrictions on movement, speech and other freedoms enjoyed by others in an unclassified

[23] At the hearing, Mr. Dennis tried to minimize the concerns that he had expressed regarding the removal of all thumb drives by NSTec. When asked whether he was upset that NSTec had taken the thumb drives away from its employees, Mr. Dennis responded, "not really." *Id.* at 221. When queried if he had complained on many occasions about the removal of the thumb drives, he replied, "not on many occasions, no." *Id.* It was my impression from observing Mr. Dennis' demeanor during his testimony about this matter that he was not candid.

environment. Trust must exist among supervisors and subordinates and co-workers to ensure those charged with missions relating to national security and the common defense function at high levels and with minimal risk of security breaches. Whether Mr. Dennis deliberately or negligently engaged in the behaviors that caused NSTec to raise "red flags" well in advance of the protected disclosure at issue in this proceeding is not relevant. In looking at the strength of NSTec's reason for the personnel action excluding the whistleblowing, I find that NSTec's contention that it terminated Mr. Dennis because it lost "trust" in him is supported by the evidence. [24]

As for the second factor set forth in *Kalil, i.e.*, the strength of any motive to retaliate for the whistleblowing, there is no direct evidence in the record of any such motive on NSTec's part.

Finally, with regard to the third factor set forth in *Kalil, e.g.*, evidence of similar action against similarly situated employees, NSTec's President testified that he had never terminated an employee because of concerns relating to national security before, but had for "comparable reasons in other areas." *Id.* at 453. He then related that the company had terminated a manager for bullying in the workplace. He also stated that there were similar cases where he made the decision that he could no longer trust an individual, and dismissed him. The Manager of Employee Relations at the time Mr. Dennis was terminated testified that there were other occasions when NSTec's behaviors resulted in termination as "the immediate and only discipline." *Id.* at 467. The first example provided was a situation where an employee was involved in a car accident at the work site and was required to take a drug screen. Id. When the individual's drug screen came back positive, NSTec immediately terminated the employee for having come to work with drugs in his system. *Id.* The second example occurred when an employee arrived at work with a weapon in his vehicle. *Id.* at 468. Rather than turning the weapon into security, the employee took the bullets out of the gun, put the bullets in the glove box of the vehicle, and the gun in the trunk. *Id.* Upon exiting the work site, the car was randomly searched and the gun and bullets found. *Id.* NSTec immediately terminated the employee. In the end, while there does not appear to have been any employee similarly situated to Mr. Dennis, NSTec did introduce evidence that it has disciplined other employees through immediate termination when it deemed conduct to be so serious that it resulted in management losing "trust" in an employee.

Considering all the relevant factors as applied to the evidence discussed above, I am convinced, based on Mr. Dennis' conduct that pre-dated his protected disclosure, that NSTec would have terminated him regardless of whether he had raised the issue of the alleged unauthorized tracking computer software. Therefore, I find that NSTec has

---

[24] The FIE Director testified that the DOE informed NSTec that it would no longer support Mr. Dennis working in the SCIF based on information provided to the agency by NSTec. Assuming this uncorroborated assertion is true and that NSTec had no other positions for Mr. Dennis, these facts would justify the personnel action taken by NSTec against Mr. Dennis. *See* David L. Moses, Case No. TBH-0066 (2008) (NNSA refused to continue funding Mr. Moses in his position because of his disruptive behavior in the workplace.)

proven, by clear and convincing evidence, that NSTec would have terminated Mr. Dennis in the absence of his protected disclosure.

V. Conclusion

As set forth above, I have determined that Mr. Dennis made one protected disclosure and has proven by a preponderance of evidence that the protected disclosure was a contributing factor to his termination. I determined, however, that NSTec has provided clear and convincing evidence to demonstrate that it would have terminated Mr. Dennis even if he had not made his protected disclosure. In conclusion, I find that Mr. Dennis has failed to establish the existence of any violations of the DOE's Contractor Employee Protection Program for which relief is warranted under Part 708.

It Is Therefore Ordered That:

(1) The Request for Relief filed by Dean P. Dennis under 10 C.F.R. Part 708 is hereby denied.

(2) This is an Initial Agency Decision, which shall become the Final Decision of the Department of Energy unless, within 15 days of the issuance of this Decision, a Notice of Appeal is filed with the Office of Hearings and Appeals Director, requesting review of the Initial Agency Decision.

Ann S. Augustyn
Hearing Officer
Office of Hearings and Appeals

Date: February 12, 2009