



**Department of Energy**  
**National Nuclear Security Administration**  
Washington, DC 20585

September 28, 2007

OFFICE OF THE ADMINISTRATOR

CERTIFIED MAIL  
RETURN RECEIPT REQUESTED

Mr. S. Robert Foley, Jr.  
Vice President - Laboratory Management  
University of California  
1111 Franklin St.  
Oakland, CA 94607

EA-2007-02

Subject: Final Notice of Violation

Dear Mr. Foley:

Pursuant to section 234B of the Atomic Energy Act of 1954, as amended, and the Department of Energy's regulations at 10 C.F.R. §§ 824.4(a)(3) and 824.7(b), the National Nuclear Security Administration (NNSA) hereby issues the enclosed Final Notice of Violation (FNOV) to the University of California. The FNOV finds the university liable for violations of DOE requirements concerning the protection of classified matter during the University of California's tenure as the management and operating contractor at Los Alamos National Laboratory (LANL). The FNOV assesses a civil penalty against the university of \$3,000,000 for these violations.

The findings set forth in the FNOV are based upon investigation of the unauthorized reproduction and removal of classified matter from LANL discovered in October 2006; evaluation of the evidence in this case, which fully supports the FNOV's determination that deficiencies in the security controls established and implemented by the university at LANL resulted in the violation of DOE classified information security requirements; and consideration of the University of California's written submissions to DOE on April 13 and April 30, 2007, in response to DOE's investigative report on the thumb drive security incident and on August 29, 2007, in response to the Preliminary Notice of Violation that NNSA issued to the university on July 13, 2007.

Pursuant to 10 C.F.R. § 824.7(d)(2), the University of California must, within 30 calendar days of its receipt of this FNOV, submit to the Director of the Office of Enforcement one of the following:

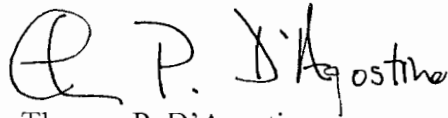
- (a) A waiver of further proceedings;
- (b) A request for a hearing under 10 C.F.R. § 824.8; or



(c) A notice of intent to proceed under section 234A.c.(3) of the Atomic Energy Act (42 U.S.C. § 2282a.(c)(3)).

The university's submittal must comport with the requirements of the Atomic Energy Act and DOE's regulations at 10 C.F.R. Part 824.

Sincerely,

A handwritten signature in black ink that reads "T. P. D'Agostino". The signature is written in a cursive style with a large initial "T" and "P".

Thomas P. D'Agostino  
Administrator

Enclosure: Final Notice of Violation, EA-2007-02

cc: B. Koonce, University of California  
B. Eklund, University of California  
T. Owens, University of California

## **Final Notice of Violation**

University of California  
Los Alamos National Laboratory

EA-2007-02

The Department of Energy (DOE) conducted an investigation of the facts and circumstances surrounding the discovery, in October 2006, of the unauthorized downloading, reproduction and removal of classified matter by an employee of a subcontractor conducting a classified information scanning project at the Los Alamos National Laboratory (LANL). The investigation identified violations of DOE classified information protection requirements contained in the DOE 470.4 series of manuals. Based on investigation of the security incident, evaluation of the evidence in this matter, and consideration of information the University of California (UC) submitted to DOE during an enforcement conference on April 13, 2007, and supplemental written material submitted on April 30, 2007, the DOE's National Nuclear Security Administration (NNSA) determined that UC is responsible for some of these violations, and issued a Preliminary Notice of Violation (PNOV) including a proposed civil penalty on July 13, 2007.

UC's response to NNSA's PNOV was received by DOE's Director of the Office of Enforcement on August 29, 2007. In that response, UC denied that it committed any violations of DOE requirements regarding the protection of classified information. It also asserted a number of arguments in support of its position that NNSA should eliminate the entire penalty proposed in the PNOV.<sup>1</sup>

NNSA thoroughly considered all of the materials submitted by UC. NNSA has determined that nothing in the materials submitted by the university justifies withdrawal of any of the violations set forth in the PNOV or a reduction in the proposed penalty. Pursuant to section 234B of the Atomic Energy Act of 1954 and sections 824.4(a)(3) and 824.7(b) of DOE regulations at 10 C.F.R. Part 824, NNSA hereby issues this Final Notice of Violation (FNOV), which imposes a

---

<sup>1</sup> NNSA addressed in the PNOV the objections UC advanced in its April 13 and April 30, 2007, written responses to DOE's investigative report of the thumb drive security incident. With respect to UC's August 29, 2007, response to the PNOV, NNSA addresses UC's violation-specific objections in Sections I.-V. below; UC's general objections to the PNOV are addressed in the Appendix attached hereto.

civil penalty of \$3,000,000 for five violations of DOE's classified information security requirements.

Section 824.4(3) of Part 824 authorizes the Department to take enforcement action and impose civil penalties for violations of classified information protection requirements in "[a]ny other DOE regulation or rule (including any DOE order or manual enforceable against the contractor or subcontractor) under a contractual provision." The DOE 470.4 series of manuals (Safeguards and Security Program) were made part of the UC contract on October 11, 2005, and UC was required to comply with them by February 26, 2006. These manuals contain the same classified information protection requirements as contained in the prior DOE manuals that had been part of the UC contract for several years.

### **Summary of Violations**

NNSA finds that UC committed the following violations. The investigative findings that underlie the violations asserted in this FNOV are set forth in the Investigation Summary Report, *Unauthorized Reproduction and Removal of Classified Matter from Los Alamos National Laboratory* (April 2, 2007), hereinafter referred to as the "Investigation Summary Report," which was transmitted to UC on April 3, 2007.

1. Violation of Requirements to Prevent, Detect, or Deter Unauthorized Access to Classified Information - UC failed to correct a known vulnerability to prevent unauthorized access to and copying of classified information from LANL's classified information systems. (See Violations, Section I.)
2. Violation of Escorting Requirements - UC did not impose adequate escorting controls for the scanning project to deter and detect unauthorized access to classified matter and its unauthorized removal to an unsecured site. (See Violations, Section II.)
3. Violation of Physical Security Requirements - UC did not assure the performance of effective physical checks of material leaving the vault-type room (VTR) housing the scanning project or the limited area surrounding the VTR in order to prevent and detect unauthorized removal of classified matter. (See Violations, Section III.)
4. Violation of Requirements regarding Roles and Responsibilities - UC failed to establish adequate roles and responsibilities for security and oversight of the scanning project. (See Violations, Section IV.)
5. Violation of Requirements for Oversight of Subcontractors - The university's oversight of subcontractor activities was deficient in ensuring effective flowdown of and compliance with security requirements. (See Violations, Section V.)

## Violations

### I. Violation of Requirement to Prevent, Detect, or Deter Unauthorized Access to Classified Information

DOE Manual 470.4-4, *Information Security* (Chg. 1, June 29, 2007, and the prior version issued on Aug. 26, 2005) requires that:

Classified matter that is generated, received, transmitted, used, stored, reproduced, or destroyed must be protected and controlled.<sup>2</sup>

“Controls must be established to prevent, deter, and detect unauthorized access to classified matter.”<sup>3</sup>

“Classified documents must be reproduced under appropriate security conditions to preclude unauthorized access to classified information.”<sup>4</sup>

“Strategies for the protection and control of classified matter must incorporate the applicable requirements established in [Section A of DOE M 470.4-4]. In addressing the threat to Departmental assets, emphasis must be placed on security systems that will prevent, detect, or deter unauthorized disclosure or modification, loss of availability, and unauthorized removal of classified matter.”<sup>5</sup>

In addition, DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management* (Chg. 1, Mar. 7, 2006, and the prior version issued on Aug. 26, 2005), requires that “[s]ecurity systems must be used that prevent, detect, or deter unauthorized access, modification, or loss of classified information or matter ... and its unauthorized removal from a site or facility.”<sup>6</sup>

In violation of these requirements, UC failed to provide and implement effective controls and security systems to prevent or deter unauthorized access to and copying of classified information from a classified LANL system as described below:

A. In the VTR used for the scanning project, data ports on the scanning project computers were used by a subcontractor’s employee to perform unauthorized downloading of classified

---

<sup>2</sup> DOE M 470.4-4, Section A, ¶ 1.a.

<sup>3</sup> *Id.* at Section A, ¶ 2.d.

<sup>4</sup> *Id.* at Section A, Chapter II, ¶ 5.b.(1).

<sup>5</sup> *Id.* at Section A, Chapter I, ¶ 4.a.

<sup>6</sup> DOE M 470.4-1 at Attachment 2, Part 1, Section A, ¶ 2.c.(3)(e).

documents onto a personally owned universal serial bus (USB)-based memory device, or “thumb drive,” after UC’s tenure as the LANL management contractor. Similar vulnerabilities were identified during UC’s tenure as the contractor. In 1999, a series of significant incidents of security concern resulted in a stand-down of operations at three weapons laboratories, including LANL. UC and the contractors for the other laboratories developed corrective action plans containing measures to make it more difficult for an insider to inadvertently or surreptitiously download classified information from a classified system to an unclassified system. One of these measures was port disablement, which UC identified as a requirement, implemented via internal policy, and inserted in its corrective action plan in accordance with the Secretary of Energy’s orders regarding this stand-down. In response to a finding from an Office of Independent Oversight inspection in September 1999, a LANL Deputy Laboratory Director required laboratory line managers to validate that all unused ports on systems accredited to process classified information were physically disabled at the hardware level or provided with tamper-indicating devices (TIDs). As part of this corrective action, UC also adopted an initiative to eliminate as many data ports as possible by replacing classified stand-alone computer systems and networks with computer technology that has no ports at the users’ terminals. Where ports could not be disabled or eliminated for operational reasons (*e.g.*, where they were needed for authorized downloading and uploading), access was to be physically controlled. Port disablement and control were incorporated into the laboratory’s Information Systems Security Officer Annual Refresher Training and remained there through UC’s tenure. In summary, uncontrolled data ports on classified computer systems were a known vulnerability during UC’s tenure at LANL. By leaving USB ports unsecured in the VTR where the thumb drive security incident occurred, UC violated the above requirements by failing to take adequate measures to address a known vulnerability and prevent unauthorized removal of classified information.<sup>7</sup>

- B. Prior to the 2006 thumb drive security incident, the UC cyber security group recognized potential vulnerabilities related to uncontrolled input/output (I/O) computer access, including USB-based memory devices and other portable media. These concerns and some proposed corrective actions were documented in a March 2006 presentation entitled *Systems Input/Output (I/O) Security* prepared by the LANL Cyber Security Contingency Planning Coordinator. This review concluded, as noted in the March 2006 presentation, that USB ports needed to be disabled on approximately 1,000 out of 2,000 classified networked systems, 350 classified stand-alone desktop systems, and 100 classified laptop systems. Proposed options for controlling ports included applying TIDs, installing certain software controls, and ensuring physical removal or disabling of the port or device. Although UC had evaluated these I/O security concerns and identified the need for corrective actions, UC did not implement these actions in the VTR between March 2006, when the need for them was identified, and May 31, 2006, when UC’s contractual responsibility for managing LANL ended.<sup>8</sup>

---

<sup>7</sup> Investigation Summary Report at 29, 47-50. The statement at page 47 that the material in Appendix B “does not form the basis for any potential enforcement action” is incorrect.

<sup>8</sup> *Id.* at 28.

- C. To prevent unauthorized access to classified information, locks were present on the computer rack cages in the subject VTR; however, the cages were not locked during UC's tenure as LANL's management contractor. Even though UC knew of the vulnerabilities posed by unprotected ports on classified systems, it did not ensure adequate physical security controls.<sup>9</sup>
- D. The configuration of the equipment for the scanning project included a classified printer. Although the subcontractor employee who duplicated and removed classified material without authorization did not require the printer to perform her assigned duties, this individual was provided access to the classified printer by UC by virtue of the default configuration of the individual's workstation in the VTR. The employee's need to access the printer was never formally reviewed by the UC scanning project leads at the start of the project. This access provided the means for the subcontractor employee to reproduce hundreds of pages of classified material.<sup>10</sup>

In its response to the PNOV, the university alleges that the lack of a specific requirement to disable data ports in a DOE manual forecloses NNSA from penalizing UC for failing to do so. As set forth above, DOE Manual 470.4-4 contains explicit requirements that contractors must protect stored classified matter, and must impose controls to prevent unauthorized access to such classified matter.<sup>11</sup> While both DOE Manuals 470.4-4 and 470.4-1 state that contractors must take a "graded approach to protection" of classified matter, they give specific direction on how contractors must develop approaches that are appropriately graded:

By a graded approach, DOE intends that, when developing and implementing protection and control programs, the level of effort and magnitude of resources expended for the protection of a particular S&S interest *should be commensurate with its importance or the effect of its loss, theft, compromise and/or unauthorized use. Interests whose loss, theft, compromise and/or unauthorized use would have serious impacts on National security . . . must be given the highest level of protection . . . .* The results of asset valuations, threat analyses, and *vulnerability assessments should be considered . . . to determine the level of risk and what protections are to be applied.* The process and results of these and other methods used to determine risk and associated mitigation strategies must be documented . . . .<sup>[12]</sup>

---

<sup>9</sup> *Id.* at 50; *see also* the LANL Security Inquiry Team Report (Jan. 18, 2007) at 16, which found that from January to November 2006, the computer rack cages were never locked.

<sup>10</sup> Investigation Summary Report at 16-17.

<sup>11</sup> DOE M 470.4-4, Section A, ¶ 2.a. and d.

<sup>12</sup> *Id.* at Section A, ¶ 7 (emphases added); *see also* DOE M 470.4-1, Attachment 2, part 1, Section A, ¶ 2.d. and e.

UC identified unsecured ports on classified systems as a significant vulnerability as early as 1999, developed corrective actions, but failed to implement them. It has presented no evidence that disabling ports on the classified computer systems, locking the racks in which the servers were located, or denying access to the classified printer would have required an excessive level of effort or resources. The information stored on the classified system used for the scanning project would have serious impacts on national security if compromised. UC cannot credibly assert that its failure to take these actions was the result of a documented graded approach to protecting classified matter of significance to national security.

UC's failure to impose adequate controls on data ports and computer racks to prevent, detect and deter unauthorized access to classified information as described above constitutes a Severity Level I violation.<sup>13</sup>

## II. Violation of Escorting Requirements

DOE Manual 470.4-2, *Physical Protection* (Chg. 1, Mar. 7, 2006, and the prior version issued on Aug. 26, 2005), requires that “[a]ccess to classified matter must be limited to persons who possess appropriate access authorization and who require such access (need to know) in the performance of official duties. Controls must be established to detect and deter unauthorized access to classified matter.”<sup>14</sup> Also, DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management* (Chg. 1, Mar. 7, 2006, and the prior version issued on Aug. 26, 2005), requires that “[s]ecurity systems must be used that prevent, detect, or deter unauthorized access, modification, or loss of classified information or matter ... and its unauthorized removal from a site or facility.”<sup>15</sup>

As discussed above with respect to Violation I, Manuals 470.4-2 and 470.4-1 do not just identify “aspirational” DOE goals or targeted strategies as UC contends.<sup>16</sup> By their express terms, these Manuals impose affirmative performance mandates on contractors, and UC was required to fulfill them.<sup>17</sup> In violation of both Manuals’ requirements, UC did not develop or impose security controls for the scanning project that were adequate to satisfy the requisite standard: to prevent, detect, and deter unauthorized access to classified matter and its unauthorized removal

---

<sup>13</sup> Appendix A of 10 C.F.R. Part 824, *General Statement of Enforcement Policy*, Section V, defines a Severity Level I violation as a violation “of classified information security requirements which involve actual or high potential for adverse impact on the national security.”

<sup>14</sup> DOE M 470.4-2, Section A, Chapter II, ¶ 11.d.

<sup>15</sup> *Id.*, Attachment 2, Part I, Section A, ¶ 2.c.(3)(e).

<sup>16</sup> UC Post-PNOV Response at 2 and Section 1-4.

<sup>17</sup> The 91-page DOE Manual 470.4-2 states (at 1) its purpose as follows: “This Manual establishes *requirements* for the physical protection of safeguards and security (S&S) interests” (emphasis added). Similarly, the stated purpose (at 1) of the 400-page DOE Manual 470.4-1 is “[t]o establish program and planning *management requirements* for the Department’s Safeguards and Security (S&S) Program” (emphasis added).



to an unsecured site. The scope and severity of UC's inadequate controls were fully revealed after UC's management responsibilities for LANL terminated, but the inadequacies existed – and persisted – during UC's tenure as LANL's M&O contractor, and it was UC that developed the specific controls for the classified information scanning project. UC violated the Manuals' requirements as follows:

- A. Based on controls established by UC, the subcontractor employee was required to be escorted while working in the VTR on the scanning project. However, notwithstanding the decision that the employee should not remain alone in the VTR, the escorts did not provide effective monitoring of the employee.<sup>18</sup>
- B. From the locations where certain escorts normally sat and performed their other work functions, the escorts could not continually maintain visual control of the subcontractor employee. Several individuals who provided occasional escort control over the employee confirmed during DOE's investigation that they could not maintain continuous visual control of the subcontractor employee.<sup>19</sup>
- C. The noise in the VTR (from the operating computing equipment) limited the effectiveness of the escort controls established by UC because the escorts could not hear if the employee used the printer; printing documents was not part of the scanning project.<sup>20</sup>
- D. UC made the determination that the project should use continuous escort controls for this subcontractor employee over a period of more than one year. As the project continued, and until the end of UC's responsibility for managing LANL, no changes were made to compensate for the limitations inherent in relying on continual escort controls.<sup>21</sup>
- E. After UC completed its tenure as LANL's management contractor, the escorting controls UC had established when it was the management contractor were demonstrated to be deficient in preventing the loss and unauthorized removal of classified information from a facility and site. A subcontract employee was able to perform multiple unauthorized tasks – downloading, printing and removing classified documents – while supposedly under the controls that had been established by UC. That the employee was able to perform these unauthorized activities on numerous occasions is evidence of the inadequacy of the controls the university had implemented.<sup>22</sup>

---

<sup>18</sup> Investigation Summary Report at 11 and 30.

<sup>19</sup> *Id.* at 30-31.

<sup>20</sup> *Id.* at 31.

<sup>21</sup> *Id.* at 30. The development of (fully anticipatable) complacency among the escorts over this one-year period, the non-routine nature of escorting a Q-cleared individual, and differing misunderstandings among the escorts of the required level of control over the subcontractor employee were all error precursors, which increased the chance of performance error.

<sup>22</sup> *Id.* at 31.

UC challenges the PNOV's findings by asserting that: no DOE escorting requirement existed because the subcontractor employee possessed a Q security clearance; the Q-cleared subcontractor employee needed access to classified information to perform her job; any breakdown in escorting controls internally imposed by UC is not a violation of DOE requirements; and all security systems are risk-based and none is infallible.<sup>23</sup> All of these assertions proceed from the flawed assumption – and fail for that reason – that UC's discretionary management decisions and actions, if not explicitly embodied in a DOE Manual requirement, cannot form the basis of a violation.

The standard UC was required to satisfy, embodied in Manuals 470.4-2 and 470.4-1, was implementation of security measures properly designed and executed to prevent the unauthorized removal of classified matter from the VTR. For the scanning project, UC designed security controls based in part on escorting requirements. Contrary to its present position, it is clear that UC did not at the time it developed the controls for the scanning project believe that the subcontractor employee's possession of a Q security clearance was alone sufficient to satisfy the requisite security standard. By UC's own admission, "it was decided" that the contractor employee should not work alone in the VTR, "primarily" because of the location there of a Classified Media Library.<sup>24</sup> It is also clear that the security controls UC determined were necessitated by virtue of establishing the contractor employee's workstation in the VTR were undermined by the failure of the resident VTR personnel to maintain continuous surveillance of that employee, whether because of visual or aural obstacles<sup>25</sup> or because of UC monetary considerations.<sup>26</sup> It is the failure of the design and implementation of UC's security controls that constitutes Violation II.

The deficient escort controls for the scanning project, as described above, constitute a Severity Level I violation.

### **III. Violation of Physical Security Requirements**

DOE Manual 470.4-2, *Physical Protection* (Chg. 1, Mar. 7, 2006, and the prior version issued on Aug. 26, 2005), requires that "[a]ccess control systems and entry control points must provide positive control that allows the movement of authorized personnel ... while detecting and delaying entry of unauthorized personnel, prohibited and controlled articles, and unauthorized removal of S&S [Safeguards and Security] interests."<sup>27</sup> Paragraph 4.c of this chapter requires that "personnel, vehicles, and hand-carried items, including packages, briefcases, purses, and lunch containers, are subject to exit inspections to deter and detect unauthorized removal of

---

<sup>23</sup> UC Post-PNOV Response at 4-5, Section 1-4 to 1-5, and Section 2-9 to 2-11.

<sup>24</sup> *Id.* at Section 2-10.

<sup>25</sup> Investigation Summary Report at 30-31.

<sup>26</sup> UC Post-PNOV Response at Section 2-11.

<sup>27</sup> DOE M 470.4-2, Section A, Chapter VIII, ¶ 2.c.

classified matter ... from security areas.”<sup>28</sup> In addition, DOE Manual 470.4-4, *Information Security* (August 26, 2005), requires that controls be established to detect unauthorized access to classified information and to prevent its unauthorized removal, and that appropriate physical security be applied to each area or building – in this case, the VTR and the servers housed therein – where classified matter is handled or processed.<sup>29</sup>

UC violated these requirements by failing to establish effective physical searches and inspections to deter and detect unauthorized removal of classified matter. UC violated these requirements as follows:

- A. Over the period of its management of LANL, UC did not establish a specific physical search requirement that focused on the unauthorized removal of classified matter from the VTR.<sup>30</sup>
- B. UC did not establish an adequate process of physical searches and inspections for classified matter being removed from the VTR.<sup>31</sup>
- C. The physical search controls that UC established and maintained in place during its management of LANL were ineffective in that the subcontract worker was subsequently able to remove without detection a large quantity of reproduced classified documents, as well as an unauthorized thumb drive that contained a large quantity of classified information.<sup>32</sup>

In response to these findings, UC asserts that it had long had an approved random search policy and practice at LANL; that no random search policy can guarantee against illegal removal of classified materials; and that the subcontractor employee was trained in, but willfully failed to follow, prohibitions against unauthorized removal of classified materials from LANL.<sup>33</sup> But whatever the inherent limits of UC’s random search policy applicable to LANL generally, and notwithstanding the training the subcontractor employee received, the fact remains that UC failed to develop and implement a physical search policy expressly addressed to the specific requirements of protecting classified information in the VTR security area where classified information was housed. As the LANS Causal Analysis points out (Attachment 1 at 7):

No physical means of detecting unauthorized or inappropriate possession of classified matter (or other items) were employed *at the VTR security area*

---

<sup>28</sup> *Id.*, ¶ 4.c.

<sup>29</sup> DOE M 470.4-4, Section A.2. and Chapter III, ¶ 1.b.

<sup>30</sup> Investigation Summary Report at 32.

<sup>31</sup> Los Alamos National Security, LLC’s *Causal Analysis and Corrective Action Plan for the Thumb Drive Incident* (hereinafter LANS Causal Analysis) (Feb. 28, 2007), Attachment 1 at 7.

<sup>32</sup> Investigation Summary Report at 32-33.

<sup>33</sup> UC Post-PNOV Response at 5, Section 1-5 to 1-6, and Section 2-11 to 2-15.

*access points.* This allowed both the USB thumb drive containing classified documents and printed classified documents to be removed from the VTR undetected (emphasis added).

UC's deficient physical search measures, as described above, constitute a Severity Level I violation.

#### **IV. Violation of Requirements regarding Roles and Responsibilities**

DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management* (Chg. 1, Mar. 7, 2006, and the prior version issued on Aug. 26, 2005), requires that "[d]elegations must be documented in writing and delineate all assigned S&S [Safeguards and Security] roles, responsibilities, and authorities for the S&S program."<sup>34</sup> Paragraph 2.c(3)(e) in Attachment 2 of this Appendix requires that "[s]ecurity systems must be used that prevent, detect, or deter unauthorized access, modification, or loss of classified information or matter ... and its unauthorized removal from a site or facility."<sup>35</sup>

In violation of these requirements, UC did not establish adequate roles and responsibilities for security and oversight related to the scanning project. Regarding line management of the scanning project, the large number of LANL program organizations involved in the project created confusion about who was responsible for project management and security.<sup>36</sup> The subsequent causal analysis of the incident conducted by LANS concluded that management responsibility for the project was diffuse, in that "no single LANL individual was responsible and accountable for assuring that security risks were comprehensively evaluated and mitigated with appropriate controls documented in the contract and work documents."<sup>37</sup> The investigation noted that several individuals had observed instances of unusual behavior by the subcontractor employee that caused them to raise concerns as to her reliability and suitability.<sup>38</sup> The LANS causal analysis concluded that the failure to address these concerns about the employee's behavior was in part due to the absence of a clear designation of a line manager who was responsible for the security of the scanning project.<sup>39</sup>

UC's contention that the Los Alamos Site Office's Contracting Officer's Representative did not expect UC to comply with the Manual 470.4-1 beginning February 26, 2006, by virtue of the

---

<sup>34</sup> DOE M 470.4-1, Attachment 2, Part 1, Section A, Appendix 1, ¶ 3.

<sup>35</sup> *Id.*, ¶ 2.c(3)(e).

<sup>36</sup> Investigation Summary Report at 35.

<sup>37</sup> *Id.*; LANS Causal Analysis, Attachment 1 at 4-5.

<sup>38</sup> Investigation Summary Report at 2 and 55.

<sup>39</sup> *Id.* at 55; LANS Causal Analysis, Attachment 1 at 8.

transition to the new contract<sup>40</sup> is not a cognizable defense to the violation charged here. *See* Section VI.C. below. UC's other contentions are also unavailing. For example, the fact that UC had written delegations in place for roles and responsibilities does not, by itself, establish that those delegations were effective in achieving the level of required performance; the inadequacy of UC's procedures constitutes a failure of UC management. Similarly, UC's assertions that the Manual does not require centralization of responsibility in a single individual, does not bar confusion, and does not dictate in precise detail how the Manual's requirements are to be met – while factually correct – do not establish any inadequacy in the standard of conduct required by the Manual or otherwise refute the finding that UC's procedures violated this standard.<sup>41</sup>

UC's deficient delineation of roles and responsibilities for the scanning project, as described above, constitutes a Severity Level I violation.

## **V. Violation of Requirements regarding Oversight of Subcontractors**

DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management* (Chg. 1, Mar. 7, 2006, and the prior version issued on Aug. 26, 2005), mandates that “[a]ffected contractors are also responsible for flowing down the requirements of the CRD [Contractor Requirements Document] to subcontracts at any tier to the extent necessary to ensure the contractors’ compliance with the requirements. ... [C]ontractors will ensure that they and their subcontractors comply with the requirements of the CRD....”<sup>42</sup>

In violation of this requirement, UC's oversight of subcontractors' activities was deficient in that it failed to ensure compliance with security requirements by its subcontractors as follows:

- A. It was generally intended that the University Technical Representatives (UTRs) oversee the subcontractors' performance, including compliance with the terms and conditions. However, roles and responsibilities were neither fully established for nor understood by the UTRs to ensure that this function was performed effectively.<sup>43</sup> According to the university's response to the PNOV, the UTR responsible for oversight of the subcontractor employee involved in the security incident did not have access to the VTR.<sup>44</sup>
- B. The LANS Security Action Team, established immediately after the security incident, concluded that there was a lack of clarity in the security language used in subcontracts. In

---

<sup>40</sup> UC Post-PNOV Response at 5 and Section 2-16.

<sup>41</sup> *Id.* at Section 1-6 to 1-7.

<sup>42</sup> DOE M 470.4-1, Attachment 2 at 1.

<sup>43</sup> Investigation Summary Report at 36.

<sup>44</sup> UC Post-PNOV Response at Section 2-21.

addition, very few UTRs understood the security requirements associated with their respective subcontracts.<sup>45</sup>

- C. LANL subcontractors were neither aware of, nor were they requiring their employees and their lower-tier subcontractors to comply with, the applicable security requirements in their subcontracts or purchase orders. Many of the existing subcontractors at LANL were hired during the tenure of UC.<sup>46</sup>
- D. LANL lacked a robust oversight program to monitor subcontractors' security program performance and implementation.<sup>47</sup>
- E. The subcontractor whose employee was involved in the security incident and other subcontractors of the university failed to submit Operations Security plans (OPSEC plans) as required by their contracts for the work they performed.<sup>48</sup>

As noted in the investigation report, these deficiencies were not limited to the subcontractor involved in the scanning project, and the basis of this violation is therefore broader than that subcontract. As to this violation, the university is being cited for its failure to devote adequate attention to security matters in its subcontracting.

In its response to the PNOV, UC first asserts the appropriate security clauses were included in the contract for the scanning project.<sup>49</sup> While that is correct, more is needed to satisfy this requirement. The university must ensure compliance with those clauses. It failed to require that subcontractors submit their OPSEC plan. UC then goes on to admit that the UTR for this project did not have access to the VTR in which the scanning project was performed, and that “[o]nce it was clear that the [employee] was proficient in her duties the degree of oversight lessened.”<sup>50</sup> As an initial matter, these statements are poor rationales for withdrawing this violation or reducing the penalty. Second, UC spends much of its response complaining that it is being penalized for the actions of a single individual's malicious acts, while at the same time admitting it had concluded she was proficient in her duties and that the UTR for the project did not even have access to the VTR where the work was performed. While NNSA has made clear that it is holding UC responsible for the deficiencies in the development and execution of its security procedures and not the security incident itself, the university's admission that “the fact that [the subcontractor employee] was working in a VTR and using a classified workstation *made*

---

<sup>45</sup> Investigation Summary Report at 36-37.

<sup>46</sup> *Id.* at 37.

<sup>47</sup> *Id.*

<sup>48</sup> *Id.* at 39-40.

<sup>49</sup> UC Post-PNOV Response at Section 1 at 8-10; Section 2-20 and 2-21.

<sup>50</sup> *Id.* at Section 2-21.

*oversight difficult*”<sup>51</sup> evidences a fundamental, and disturbing, misunderstanding of the proper approach to security matters.

Collectively, these deficient controls in oversight of subcontractor security requirements, as set forth above, constitute a Severity Level I violation.

## **VI. Assessment of Civil Penalties**

NNSA assesses a civil penalty of \$3,000,000 for the violations identified above, in consideration of the gravity of the security breach, UC’s failure to correct the classified information security deficiencies resulting in the breach, the prior history of UC’s security management deficiencies at the laboratory, and UC’s failure to establish a basis for remission or mitigation of the penalty. NNSA also considered UC’s total disclaimer of any responsibility for the structural management failures that created the vulnerabilities that allowed the thumb drive incident to occur, which it repeated in its response to the PNOV.

### **A. Severity of the Violations**

The significance or gravity of the security breach is a central factor in assessing a civil penalty.<sup>52</sup> In this case, the classified matter unlawfully removed from LANL included data concerning nuclear weapons design and the nuclear weapons test data collection methodologies of the United States and its allies.<sup>53</sup> This information is some of the most sensitive data DOE possesses. The data included hard copy documents as well as electronic files that could have been easily distributed and copied.

The classified matter unlawfully removed, moreover, was not merely one or a few documents. It consisted of 421 document files with 1,219 pages, five .dat files, and seven Microsoft Access database files, for a total of 433 items of classified matter:

- Of the 421 document files:
  - Twenty-three documents (142 pages) were Secret/Restricted Data (S/RD) in the Sigma 1 and Sigma 2 caveats;<sup>54</sup>
  - 296 documents (802 pages) were Secret/National Security Information (S/NSI) with the No Foreign Dissemination caveat (NOFORN);<sup>55</sup>

---

<sup>51</sup> *Id.* (emphasis added).

<sup>52</sup> 10 C.F.R. Part 824, Appendix A, ¶ V.a.

<sup>53</sup> DOE M 470.4-4, Section A, Chapter II, ¶ 1.1.(4)(a); Investigation Summary Report at 6 and documents cited in n.23 thereof.

<sup>54</sup> Sigma 1 concerns the theory of operation (hydrodynamic and nuclear) or complete design of thermonuclear weapons or their unique components. Sigma 2 concerns the theory of operations or complete design of fission weapons or their unique components. The latter includes the high explosive system with its detonators and firing unit, pit system, and nuclear irrigation system as they pertain to weapons design and theory.

- Sixty-six documents (199 pages) were S/NSI without caveat;
  - Four documents (eleven pages) were Confidential/National Security Information (C/NSI); and
  - Thirty-two documents (sixty-five pages) were Unclassified.
- Of the five .dat files:
    - One .dat file was S/NSI without caveat; and
    - Four .dat files were Unclassified.
- Of the seven Microsoft Access database files:
    - Three were S/RD;
    - Three were Unclassified; and
    - One could not be opened.

Severity Level I violations are defined in paragraph V.b of DOE’s General Statement of Enforcement Policy (hereinafter “Enforcement Policy”) as “the most significant,” a designation reserved for violations of classified information security requirements “which involve actual or high potential for adverse impact on the national security.” The Investigation Summary Report (at 25-42) discusses the inadequate management control system – established and implemented during UC’s tenure as LANL’s management contractor – that created the deficiencies that led to the security breach: deficient controls to protect and prevent access to classified matter, inadequate implementation of escort controls to prevent unauthorized access to classified computers and a printer, and poor line-management oversight of subcontractors.

## B. Potential Penalties

As discussed in Sections I.-V. above, NNSA has determined that all of the violations identified herein constitute Severity Level I violations, the most serious category of violations. In accordance with section 234B.a. of the Atomic Energy Act, of 1954, as amended, and under DOE’s Enforcement Policy, each Severity Level I violation is subject to a maximum base civil penalty of \$100,000 per day. UC’s violations existed from the first day of its required compliance with the DOE security manuals, February 26, 2006, and continued through the remaining period of UC’s management of LANL, which ended on May 31, 2006. Thus, the violations continued for a period of 94 days.

For certain contractors (including UC), the total amount of penalties in a fiscal year may not exceed the total amount of fees paid by DOE to the contractor in the fiscal year in which the

---

<sup>55</sup> The “NOFORN” designation is used for information that may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without the originator’s approval.



violations occurred.<sup>56</sup> NNSA paid UC \$5.8 million in fees for FY2006. Thus, the total available civil penalty “pool” applicable to the violations alleged herein is limited to \$5.8 million, which is far below the otherwise maximum permissible penalty of 94 days multiplied by \$500,000 (\$100,000 x 5 violations).

### C. Mitigation of Penalties

At the April 13, 2007, enforcement conference, and in its written submissions to the Department’s Office of Enforcement provided at the conference and subsequently (April 27 and August 29, 2007), UC disclaimed all responsibility for the security breach on the grounds that the subcontractor employee, not UC, committed the security breach; and that UC was not the LANL management contractor at the time the misappropriation of classified matter was discovered. In its April 27 submission, UC also asserted 11 factors in whole or partial mitigation of the imposition of civil penalties. In this regard, UC contended that it and DOE rely on complementary systems to protect classified information; UC acted to prevent security incidents and strengthen Accountable Classified Removable Media (ACREM) accountability; UC used expert advisors, engineered tools, and forums to strengthen LANL security practices; the Red Network expansion represents the best solution to prevent the transfer of classified information to unclassified computing systems; UC’s Integrated Safeguards and Security Management (ISSM) implementation provided workers with guidance, training, and tools to operate more securely; and UC management continued to improve ISSM implementation through the last day of UC’s tenure as the contractor (May 31, 2006).

These assertions are misdirected and unavailing. First, UC is responsible for its structural management deficiencies; it may not escape liability for those deficiencies because an individual subcontractor employee exploited weaknesses in UC’s security management controls shortly after the university’s tenure ended. Furthermore, the gravamen of UC’s violations is not the entire absence of security controls, or that UC failed to take any corrective actions to remedy security deficiencies at LANL. Rather, NNSA finds that UC did not have adequate management processes in place to prevent the thumb drive incident, even though simple corrections could have prevented it.<sup>57</sup>

UC has also asserted in mitigation that the subcontractor employee involved in the thumb drive incident was well trained to protect and handle classified information, and that LANL policy

---

<sup>56</sup> 42 U.S.C. § 2282b; 10 C.F.R. § 824.2(b).

<sup>57</sup> One illustrative example will suffice: UC determined that the media storage racks need not be locked because the racks did not contain classified removable media (CREM) and were located inside a VTR, and that only employees permitted access to the media storage devices would permanently reside in the VTR. All others granted access to the VTR would be non-privileged employees who would be properly escorted and continuously monitored, and thereby denied access to the unlocked device storage racks. However, UC introduced a non-privileged subcontractor employee into the VTR on a “temporary” basis lasting more than a year. This temporary/permanent residency eviscerated the security controls of the VTR because it permitted the very circumstance the policy sought to protect against – access to the storage racks by a non-privileged employee without authorized access. Locking the racks to preclude downloading of classified data, which UC did not do, was required to and could have prevented the thumb drive incident.

made workers responsible for implementing all applicable security requirements. UC cannot so casually divorce itself from responsibility for acts of subcontractor employees. DOE's Enforcement Policy states that DOE will take into consideration "the position, training and experience of the person involved in the violation."<sup>58</sup> The fact that the subcontractor employee acted willfully despite her training does not excuse or mitigate UC's liability for its management deficiencies. As stated in the Enforcement Policy:

[W]hile management involvement, direct or indirect, in a violation may lead to an increase in the severity of a violation and proposed civil penalty, the lack of such involvement will not constitute grounds to reduce the severity level of the violation or mitigate a civil penalty. Allowance of mitigation in such circumstances could encourage lack of management involvement in DOE contractor activities and a decrease in protection of classified information.<sup>[59]</sup>

UC next asserted that DOE and NNSA rated as "effective" UC safeguards and security performance, with only a few exceptions. Neither DOE regulations nor the Enforcement Policy recognize past performance ratings as mitigating factors in an enforcement action, and the particular circumstances of this case do not warrant excusing or reducing the civil penalty assessment on the basis of such ratings.

UC claimed that NNSA accepted increased security risks because of budget reductions, and that the Los Alamos Site Office (LASO) agreed to delay implementation of the DOE 470 series of manuals until FY2007 because of budget and transition issues. However, the Department's Enforcement Policy expressly provides that:

DOE does not consider an asserted lack of funding to be a justification for noncompliance with classified information security requirements. Should a contractor believe that a shortage of funding precludes it from achieving compliance with one or more of these requirements, it may request, in writing, an exemption from the requirement(s) in question from the appropriate Secretarial Officer (SO).<sup>[60]</sup>

UC provided no evidence that it either requested, or received, an exemption from applicable classified information security requirements from the appropriate Secretarial Officer, for budgetary or other reasons.

Instead, UC asserted that three sets of Protection Program Management Team (PPMT) meeting minutes<sup>61</sup> establish that the LASO gave UC written approval -- "the equivalent of a waiver"<sup>62</sup> --

---

<sup>58</sup> 10 C.F.R. Part 824, Appendix A, ¶ V.d.

<sup>59</sup> *Id.*

<sup>60</sup> 10 C.F.R. Part 824, Appendix A, ¶ VIII.1.c.

<sup>61</sup> Materials UC presented at the April 13, 2007, Enforcement Conference, Tab 11, items H.-J.

for noncompliance until FY 2007 with DOE Manuals 470.4-1 (*Safeguards and Security Program Planning and Management*) and 470.4-4 (*Information Security*). This claim is baseless (even assuming *arguendo* the probative value of such minutes as evidence of waiver of DOE's classified information protection requirements). The portion of the September 21, 2005, PPMT minutes UC highlights contains no mention of any Departmental directives. The October 26, 2005, PPMT minutes cite "some disruption with readiness assessment activities" – a reference to LASO activities concerning the transition to a new LANL M&O contractor, not to UC's obligations to maintain the security of classified information. The reference in the April 20, 2006, PPMT minutes to a delay by 2 months of the submission of an implementation plan for the "streamlined directives" and "full implementation of directives . . . into FY07" is a statement by a UC/LANL employee, not LASO's written approval of UC's noncompliance with DOE security directives.

DOE's Enforcement Policy states that DOE will provide substantial incentive through mitigation of civil penalties based on timely self-identification and reporting of violations, and timely and effective corrective actions for those violation conditions (at sections VIII.3, VIII.4, VIII.5, VIII.6 and VIII.7). The violation conditions in this case were clearly discoverable, were not identified, reported, and corrected by UC in a timely manner during its tenure as the management contractor, and were disclosed by the subsequent investigations in response to the security breach discovered in October 2006.<sup>63</sup> Thus, UC cannot receive credit for mitigation under these sections of DOE's Enforcement Policy.

In its August 29, 2007, response to the PNOV, UC re-asserts all of the foregoing defenses, adding "DOE's role in the violation" as "[a]dditional [r]elevant [i]nformation" expressly denominated as "a consideration for penalty mitigation."<sup>64</sup> Specifically, UC asserts that the circumstances surrounding NNSA's decision to grant the subcontractor employee a Q security clearance "calls into question" NNSA's responsibility for the security incident. *Id.* This variation on UC's repeated attempts to deflect attention from its own to others' actions is as unpersuasive as its other attempts in this regard. UC is not charged in this enforcement proceeding with a violation originating from the security incident itself. Therefore, it is irrelevant whether UC was aware of any "derogatory information" concerning the subcontractor employee, or whether NNSA's role in granting her a clearance should be a mitigating factor in such a violation. *Id.* Rather, UC is being held responsible here only for the deficiencies of its management procedures and practices related to the protection of classified information involved in the scanning project.

In sum, NNSA finds no basis for remission or mitigation of civil penalties based on UC's asserted defenses.

---

<sup>62</sup> *Information Provided by the University of California to Supplement Enforcement Conference Materials dated April 13, 2007* (April 27, 2007) at 19.

<sup>63</sup> Investigation Summary Report at 38-39.

<sup>64</sup> UC Post-PNOV Response at Section 3-1.

#### D. Civil Penalty

A substantial penalty is fully warranted in this case. While civil penalties assessed under 10 C.F.R. Part 824 should not be unduly confiscatory, they should nonetheless be commensurate with the gravity of the violations at issue. In this regard, NNSA considered the nature, number, and Severity Level of the violations found here as well as the circumstance of the case. These circumstances included the transition from UC to LANL's new management contractor and the proximity in time of the security incident to that transition, and determined not to seek imposition of the maximum permissible penalty of \$5.8 million. At the same time, however, NNSA also considered LANL's history over the last decade under UC's management of similar security program deficiencies as those leading to the October 2006 security incident. UC's written presentation materials at the April 13, 2007, enforcement conference acknowledged these deficiencies, citing "repeated and embarrassing security incidents" (at 3) involving ACREM.

In addition, while civil penalties should deter future violations by encouraging corrective remedial actions, civil penalties are intended to exact a penalty for serious violations. Thus, the fact that UC is no longer LANL's management contractor, and in fact has sought to evade its responsibility on unpersuasive grounds, does not constitute a persuasive basis to remit or mitigate the penalty assessment here.<sup>65</sup> In consideration of the gravity of the security breach, the particular circumstances of this case, and UC's failure to establish the existence of factors for mitigation, NNSA assesses a civil penalty of \$3,000,000.

#### **Required Response**

Pursuant to the provisions of 10 C.F.R. § 824.7(d)(2), UC must, within 30 calendar days of receipt of this FNOV, submit to the Director of the Office of Enforcement one of the following:

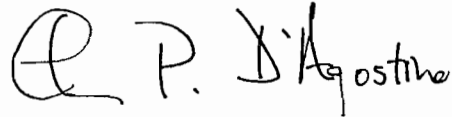
- (a) A waiver of further proceedings;
- (b) A request for an on-the-record hearing under 10 C.F.R. § 824.8; or
- (c) A notice of intent to proceed under section 234A.c.(3) of the Act, 42 U.S.C. § 2282a.(c)(3).

UC's reply to the FNOV shall be directed via overnight carrier to the Director, Office of Enforcement, Attention: Office of the Docketing Clerk, HS-40/270 Corporate Square Building, U.S. Department of Energy, 19901 Germantown Road, Germantown, MD 20874-0270. Copies of any reply should also be sent to the Manager of the Los Alamos Site Office and to the Office of the Administrator, National Nuclear Security Administration. The reply shall be clearly marked as a "Reply to a Final Notice of Violation."

---

<sup>65</sup> UC is the management and operating contractor at the Lawrence Berkeley and Lawrence Livermore National Laboratories, and a member of LANS and of Lawrence Livermore National Security, LLC, which will assume the role of management and operating contractor at the Livermore laboratory on October 1, 2007. UC's refusal to accept responsibility for the security deficiencies revealed by this incident, or to attempt to learn from them, is very troubling.

If UC submits a waiver of further proceedings, the FNOV shall be deemed a final order enforceable against UC. UC shall submit payment of the civil penalty within 60 days of the filing of waiver unless additional time is granted. The civil penalty shall be paid by check, draft, or money order payable to the Treasurer of the United States (Account 891099) and mailed to the Director, Office of Enforcement, Attention: Office of the Docketing Clerk, at the address above.

Handwritten signature of Thomas P. D'Agostino in black ink.

Thomas P. D'Agostino  
Administrator

Washington, D.C.  
This 28th day of September 2007

## APPENDIX

### UC's General Objections to the PNOV

In response to the PNOV, the university raised a number of general objections to aspects of the PNOV. Some of these objections are addressed in this Appendix; others require only a brief mention<sup>66</sup>

#### *UC Cannot Be Held Liable Because the Security Incident Occurred After Its Tenure Ended*

The university asserts repeatedly that it cannot be held liable because the security incident occurred after its tenure had ended. These assertions are incorrect. While the investigation indicated that the security incident itself – consisting of the downloading of classified material onto a thumb drive, the printing of classified material on paper, and the removal of both from the laboratory – probably occurred after the university was no longer the M&O contractor at LANL, the PNOV clearly stated that UC was being held for failing to develop and implement adequate security procedures for the scanning project during which the incident occurred. LANS was held liable for the security incident, fined \$300,000 for the violation arising from the incident, and paid the penalty in full.<sup>67</sup> The incident and the subsequent investigation into its causes did reveal that the university's procedures for the scanning project were deficient and contributed to the causation of the incident; however, UC has not been cited for the incident or penalized for it. Therefore, UC is not being held liable for the actions of LANS, the subcontractor in charge of the scanning project, or the subcontractor's employee responsible for the incident. UC is being held responsible for its failure to impose security procedures on the project that met DOE requirements.

The university also asserts that “but for” the security incident, NNSA would never have examined the security procedures UC implemented for the scanning project and found them to be deficient. While that may be true, it is not a rationale for ignoring the deficiencies exposed by the incident or for mitigating the penalty for those violations. UC also raises the specter of NNSA imposing penalties “long after a contractor's contract with DOE has expired” “with no apparent statute of limitations.”<sup>68</sup> This concern is, as to this matter, unfounded. The incident that revealed these deficiencies occurred during the first four months after UC's tenure had ended. UC, as a member of LANS, had access to the facilities and facts relating to this incident, and does not claim that LANS changed the procedures the university had implemented for the

---

<sup>66</sup> For example, the fact that this case is the first and only university violation under 10 C.F.R. Part 824 (UC Post-PNOV Response at 3) does not bar an enforcement action and is not otherwise a cognizable defense to it. UC's assertion that the university's management engaged in no willful misconduct (*id.*) addresses a standard applicable to criminal proceedings, but not to civil enforcement actions such as this one. The fact that the subcontractor employee had a Q clearance, and a need-to-know all of the classified information found in her residence (*id.* at 5) does not excuse UC's management deficiencies which came to light as a result of the security incident uncovered in October 2006.

<sup>67</sup> DOE Enforcement Action EA 2007-01, July 13, 2007.

<sup>68</sup> UC Post-PNOV Response at Section 1-11 and 1-12

scanning project. One can construct a hypothetical in which citing a former contractor for violations “long after” its tenure has concluded would be unfair. The facts of this situation, however, allow no such assertion.

*UC Cannot Be Held Liable for Violations of “Aspirational Goals” in DOE Manuals or “Self-Imposed” Requirements*

In a number of places in its response, the university argues that some requirements in DOE Orders and Manuals are “aspirational goals” as to which the Department cannot expect “absolute assurance against failure.” UC Post-PNOV response at 2 *passim*. It also asserts that UC cannot be held liable for violations of its “self-imposed” requirements that it alleges are “more stringent” than DOE’s. *Id.* at 2. These comments reflect a fundamental misunderstanding of the regulatory regime established by DOE’s system of orders and manuals. In general, orders and manuals establish important objectives and standards that its contractors must achieve.<sup>69</sup> DOE requirements are not aspirational goals, but fundamental expectations. How these objectives and standards are met for a particular project or activity is left for the contractor to determine, with appropriate oversight from the Department. The university was responsible for developing and implementing security procedures for the scanning project that satisfied the overarching requirements set forth in DOE’s regulations, Orders and Manuals. As discussed in Sections I.-V. above, those procedures were deficient, improperly implemented, or both, with the result that UC violated DOE security requirements.

*UC Cannot Be Held Liable Because NNSA Acquiesced to the University’s Deficient Procedures and Its Implementation of Them*

The university asserts that NNSA’s Los Alamos Site Office “was fully informed at all times” about UC’s security program at LANL and that NNSA “effectively consented” to the university’s safeguards and security policies and procedures. UC Post-PNOV Response at 3 and Section 1-3. As stated in DOE’s Enforcement Policy, contractors must obtain written exemptions from security requirements or, “in conjunction with the SO [Secretarial Officer] must take appropriate steps to modify, curtail, suspend or cease the activities which cannot be conducted in compliance with the classified information security requirements in question.” DOE Manual 470.4-1 establishes formal procedures for obtaining deviations from security requirements.<sup>70</sup> The university did not obtain a written exemption, and did not modify or suspend the scanning project. Accordingly, there is no basis for the assertion that NNSA

---

<sup>69</sup> In addition to general objectives and requirements, the Manuals also contain specific requirements. But for the most part, the Manuals require contractors to develop plans and programs for the activities they conduct that will ensure these activities are performed in accordance with the overarching security requirements established in the Manuals. For example, DOE M 470.4-1 requires development of: a Safeguards and Security Management Plan (Attachment II, Part 1, Section A, ¶ 2.b); facility specific Safeguards and Security Plans (Attachment II, Part 1, Section A, ¶ 3.a); a Site Safeguards and Security Plan (Attachment II, Part 1, Section A, ¶ 3.b); and procedures for inquiry into and reporting of incidents of security concern (Attachment II, Part 2, Section N, ¶ 2.d).

<sup>70</sup> DOE M 470.4-1 at M-1 through M-8; Attachment 2 at M-1 through M-6. Other DOE Manuals incorporate the procedures in DOE Manual 470.4-1. *E.g.*, DOE M 470.4-4, *Information Security*, at iv.

consented to or acquiesced in the deficient security procedures the university implemented for this project, and therefore no basis for reduction of the penalty imposed.<sup>71</sup>

*In Calculating the Penalty, Past Security and Safety Incidents Are “Not Relevant” if They Occurred Prior to the Effective Date of 10 C.F.R. Part 824*

UC makes this assertion without any support from Part 824, the record of its promulgation, or the Enforcement Policy.<sup>72</sup> There is no support for this assertion and no sound rationale why NNSA should ignore incidents that predate Part 824 when calculating penalties. Similarly, the university argues that, because the version of DOE Manual 470.4-1 that contained the notice of civil penalties did not become effective until after planning for the scanning project had begun, UC was not required to implement it.<sup>73</sup> Again, UC provides no evidence or reason in support of its claim that requirements and penalty provisions in security manuals should be applied only to projects and activities initiated after the effective date of these provisions.

---

<sup>71</sup> This situation illustrates the sound rationale behind the requirement that contractors follow a formal procedure to obtain an exemption from security requirements. UC asserts that information provided at meetings, and the minutes of those meetings, constitute a waiver of security requirements. As discussed in the PNOV (at 10) and in Section VI.C. above, the meeting minutes cited by UC contain no mention of Departmental directives and only brief notes on what was discussed at the meetings. Cryptic notations of informal discussions would be an inappropriate way to make and memorialize decisions regarding security procedures at a nuclear weapons laboratory, as DOE’s Enforcement Policy and its Manuals clearly state.

<sup>72</sup> UC Post-PNOV Response at 3, Section 1-11 and Section 3-4.

<sup>73</sup> *Id.* at 5 and Section 2-16 through 2-17.