Department of Energy
National Nuclear Security Administration
Washington, DC 20585

July 13, 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: Preliminary Notice of Violation

Dear Mr. Foley:

The Department of Energy (DOE) has completed its investigation of the unauthorized reproduction and removal of classified matter from the Los Alamos National Laboratory (LANL) discovered in October 2006. Based on investigation of the incident and evaluation of the evidence in this matter, and in consideration of information you and members of your staff provided during an enforcement conference held on April 13, 2007, and supplemental written material submitted by the University of California on April 30, 2007, I am issuing the enclosed Preliminary Notice of Violation (PNOV), in accordance with 10 C.F.R. § 824.6. A summary of the April 13 enforcement conference is also enclosed.

As set forth in the PNOV, the DOE's National Nuclear Security Administration finds that deficiencies in the security controls established and implemented by the University of California at the laboratory during its tenure as the management contractor at LANL were a central factor in the thumb drive security breach discovered in October 2006. The enclosed PNOV details the University of California's security management deficiencies that resulted in the violation of DOE classified information security requirements, and proposes assessment of a civil penalty of $3,000,000.

This incident is particularly troubling because the violations cited in the PNOV are of the same nature as other performance deficiencies that occurred during the University of California's tenure in the areas of safety and security. As revealed by this incident and the Department's investigation, the University of California had systemic failures in establishing adequate work controls, consistently implementing these controls, assessing the effectiveness of its protection measures and improving the quality of these measures over time. The processes the University of California established for the classified information scanning project created vulnerabilities that led to the compromise and potential loss of national security information.

Pursuant to 10 C.F.R. § 824.6(a)(4), the University of California has the right to submit a written reply to the PNOV within 30 calendar days of receipt. A reply must contain a statement of all relevant facts pertaining to the violations alleged and must otherwise comply with the requirements of 10 C.F.R. § 824.6(b). Pursuant to 10 C.F.R. § 824.6(c), failure to submit a written reply within 30 calendar days constitutes relinquishment of any right to appeal any matter in the PNOV; and the PNOV, including the assessment of penalties, constitutes a final order.

.

Sincerely,

William C. Ostendorff
Acting Administrator

Enclosures: Preliminary Notice of Violation, EA-2007-02
Enforcement Conference Summary, EA-2007-02

cc: Mr. Buck Koonce, University of California
Mr. Bill Eklund, University of California
Mr. Terry Owen, University of California

Preliminary 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 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. The DOE's National Nuclear Security Administration (NNSA) has determined that the University of California (UC) is responsible for some of these violations. Pursuant to section 234B of the Atomic Energy Act of 1954, as amended, and DOE regulations at 10 C.F.R. §§ 824.4(a)(2) and 824.6(a), NNSA hereby issues this Preliminary Notice of Violation (PNOV) and proposes a civil penalty of $3,000,000 for violations of DOE's classified information security requirements.

Section 824.4(3) 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 implement them by February 26, 2006. These manuals contained the same classified information protection requirements as those contained in the predecessor DOE manuals that had been incorporated in the UC management contract for several years. The advisory regarding the imposition of civil penalties for violation of the security requirements of the 470.4 manuals, including 470.4-4 (Information Security), was applicable to UC from February 26, 2006, through the end of its tenure as the management contractor at LANL, which tenure ended on May 31, 2006.

Summary of Violations

In summary, NNSA finds that UC committed the following violations. The investigative findings that underlie the violations asserted in this PNOV 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 Requirement to Protect Data Ports - UC failed to correct a known vulnerability to prevent unauthorized access to and downloading 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 - UC 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 Protect Data Ports

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: "Security 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." *Id.* at Attachment 2, Part 1, Section A, ¶ 2.c.(3)(e).

In violation of this requirement, UC failed to correct known vulnerabilities to prevent unauthorized access to and downloading of classified information in LANL's cyber system. UC violated this requirement as follows:

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 download of classified documents onto a personally-owned universal serial bus (USB), or "thumb drive," after UC's tenure as the LANL management and operating (M&O) contractor. Similar vulnerabilities were identified during UC's tenure as the M&O 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 failed to ensure compliance with established policy in this area and failed to adequately address a known vulnerability.

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. The cyber security group concluded, as noted in the 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, the university took no action to address the concerns at LANL between March 2006, when this need for action was identified, and May 31, 2006, when UC's contractual responsibility for LANL management terminated.

C. To prevent physical access to classified systems, locks were present on the computer rack cage in the subject VTR; however, the rack was not locked. Even though UC knew of the vulnerabilities posed by unprotected ports on classified systems, it did not ensure adequate physical security controls.

The deficient protection of data ports constitutes a Severity Level I violation.[1]

II. Violation of Escorting Requirements

DOE Manual 470.4-2, *Physical Protection*, (Chg. 1, Mar. 6, 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." *Id.* at Section A, Chapter II, ¶ 11.d. 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." *Id.* at Attachment 2, Part 1, Section A, ¶ 2.c.(3)(e).

In violation of these requirements, UC did not develop or impose adequate escorting controls for the scanning project to prevent, detect and deter unauthorized access to classified matter and its unauthorized removal to an unsecured site. Many of these inadequacies were fully revealed after UC's completion of its contract period, but they were present during UC's tenure, and it was UC that developed the escorting controls for the classified information scanning project. UC violated these requirements as follows:

A. The subcontractor employee was required to be escorted while working in the VTR on the scanning project, based on the controls established by UC. However, several of the escort personnel erroneously believed that because the employee possessed a "Q" access authorization, they did not need to provide continuous monitoring —that is, the escorts believed they only needed to clear the employee into the VTR, not maintain continuous control of the employee.

B. 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.

C. 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.

D. The noise in the room (from the operating computing equipment) limited the effectiveness of the escort controls established by UC because the escorts could not

[1] 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."

hear if the employee used the printer; printing documents was not part of the scanning project.

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 when the employee was able to perform multiple unauthorized tasks — unauthorized duplication and removal of classified documents— while supposedly under the controls established by the university.

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." *Id.* at Section A, Chapter III, ¶ 2.c. 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 classified matter ... from security areas." 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 where classified matter is handled or processed. *Id.* at Section A. 2. and Chapter II, 7.j.(4).

UC violated these requirements by failing to establish effective physical searches and inspections for classified matter being removed from the subject VTR or associated limited area to prevent, detect or deter unauthorized removal of classified matter. UC violated these requirements as follows:

A. UC had not established a specific physical search requirement for LANL that focused on classified areas, prior to the thumb drive incident, over the period of UC's management of LANL.

B. 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 similarly contained a large quantity of classified documents.

These 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 roles, responsibilities, and authorities for the S&S program." *Id.* at Attachment 2, Part 1, Section A, Appendix 1, ¶ 3. Paragraph 2.c(3)(e) 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."

In violation of these requirements, UC did not establish adequate roles and responsibilities for security and oversight related to the scanning project. UC violated these requirements as follows:

A. With respect to 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. The subsequent causal analysis of the event (performed by the current contractor, Los Alamos National Security, LLC (Feb. 28, 2007)) 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."

B. With respect to Information System Security Plans (ISSPs) in general and in particular as to the secure local network in the VTR where the security incident subsequently occurred, members of the cyber security group did not typically perform walkdowns to support their review of the ISSPs the group developed.

C. Representatives of the cyber security group were not typically involved in initial and annual system testing.

Collectively, the deficient delineations of roles and responsibilities, as described above, constitute 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 [Contract Requirements Document] to subcontracts at any tier to the extent necessary to ensure the contractors' compliance with the requirements." *Id.* at Attachment 2.

In violation of this requirement, UC's oversight of subcontractor activities was deficient and failed to ensure effective flowdown and compliance with security requirements as follows:

A. Roles and responsibilities were neither fully established for nor understood by the University Technical Representative (UTR).

B. There was a lack of clarity and standardization in the security language used in subcontracts. Additionally, very few UTRs understood the security requirements associated with their respective subcontracts.

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.

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

VI. Assessment of Civil Penalties

NNSA proposes the assessment of a civil penalty of $3,000,000 for the violations identified above, in consideration of the significance of the security breach, UC's failure to correct the classified information security deficiencies resulting in the breach, and the prior history of UC's management deficiencies at the laboratory. In proposing a civil penalty in this case, 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.

A. Severity of the Violations

The significance or gravity of the security breach is a central factor in proposing the assessment of a civil penalty.[2] 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.[3] 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;
    - 296 documents (802 pages) were Secret/National Security Information (S/NSI) with the No Foreign Dissemination caveat (NOFORN);
    - Sixty-six documents (199 pages) were S/NSI without caveat;

[2] 10 C.F.R. Part 824, Appendix A, ¶ V.a.

[3] *See* footnote 1 *supra*.

- 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.

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: the failure to secure data ports in classified computer systems, inadequate implementation of escort controls to prevent unauthorized access to classified computers, and poor line-management oversight of subcontractors.

NNSA also considered the history of similar deficiencies leading to the security breach, including the number of security incidents over the last decade of UC's management of LANL. UC's written presentation materials at the April 13, 2007, enforcement conference acknowledged these deficiencies, citing "repeated and embarrassing security incidents" (at 3) involving Accountable Classified Removable Electronic Media (ACREM).

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, and under DOE's General Statement of Enforcement Policy (hereinafter "Enforcement Policy"), each Severity Level I violation is subject to a maximum base civil penalty of $100,000 per day; 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 violations occurred. 42 U.S.C. § 2282b; 10 C.F.R. Part 824, Appendix A. The Department of Energy paid UC $5.8 million in fees for FY2006. Thus, notwithstanding that the $100,000 maximum per day/per violation base penalty amount far exceeds $5.8 million, the total available civil penalty "pool" applicable to the violations alleged herein is $5.8 million.

C. Mitigation of Penalties

At the April 13, 2007, enforcement conference, and in its written submissions to the Department's Office of Enforcement both at the conference and subsequently (April 27, 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. UC also asserts 11 factors in whole or partial mitigation of the imposition of civil penalties. In this regard, UC contends that it and DOE rely on complementary systems to protect classified information; UC acted to prevent security incidents and strengthen 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 management contract (May 31, 2006).

These assertions are misdirected and unavailing. As an initial matter, 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.[4]

UC 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 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."[5] The fact that the subcontractor employee acted willfully despite her training does not excuse or mitigate UC's liability for its management deficiencies.

> [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

---

[4] 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.

[5] 10 C.F.R. Part 824, Appendix A, ¶ V.d.

> mitigation in such circumstances could encourage lack of management involvement in DOE contractor activities and a decrease in protection of classified information.[6]

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).[7]

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[8] establish that the LASO gave UC written approval -- "the equivalent of a waiver"[9] -- 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 two 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

---

[6] *Id.*

[7] 10 C.F.R. Part 824, Appendix A, ¶ VIII.1.c.

[8] Materials UC presented at the April 13, 2007, Enforcement Conference, Tab 11, items H.-J.

[9] "Information Provided by the University of California to Supplement Enforcement Conference Materials dated April 13, 2007" (April 27, 2007) at 19.

employee, not LASO's written approval of UC's noncompliance with DOE security directives.[10]

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

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 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. In addition, while civil penalties should deter future violations by encouraging corrective remedial actions, civil penalties are also intended to exact a penalty for past 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.[11] In consideration of the gravity of the security breach, the particular circumstances of this case, UC's history of prior similar violations, and UC's failure to establish the existence of factors in mitigation, NNSA proposes the assessment of a civil penalty of $3,000,000.

Opportunity to Respond

Pursuant to the provisions of 10 C.F.R. § 824.6, UC may, within 30 calendar days of receipt of this PNOV, submit a written reply to the Director of Enforcement. If such a reply is made, it should 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 20874-1290. Copies of any reply should be sent to the Manager of the Los Alamos Site Office and to the Office of the Administrator, National Nuclear Security Administration.

The reply should be clearly marked as a "Reply to a Preliminary Notice of Violation" and, in accordance with 10 C.F.R. § 824.6(b), should include the following information for each

---

[10] Finally, in its post-enforcement conference submission of April 27, 2007, UC asserted (at 17) an additional defense: that the Eleventh Amendment to the U.S. Constitution bars this enforcement action against the University as an instrumentality of the State of California. This claim is patently untenable. The Amendment bars suits in law or equity "commenced or prosecuted against one of the United States by Citizens of another State, or by Citizens or Subjects of any Foreign State." Among the threshold defects of UC's claim is the fact that the Eleventh Amendment by its plain text does not bar suits by the United States.

[11] The university is the management and operating contractor at the Lawrence Berkeley and Lawrence Livermore National Laboratories, and a member of the LANS team. UC's refusal to accept responsibility for this incident, or to attempt to learn from it, is very troubling.

violation: (1) facts or arguments that refute the PNOV's finding of violation; (2) information that demonstrates extenuating circumstances or other reasons why the proposed penalty should not be imposed or should be reduced; (3) any relevant rulings or determinations that support the positions asserted; and (4) copies of any documents cited in the reply that have not previously been provided. If no reply is submitted within 30 calendar days, in accordance with 10 C.F.R. § 824.6(c), this PNOV, including the proposed penalties, constitutes a final order.

Within 30 calendar days after receipt of this PNOV, unless the university files the reply as provided in 10 C.F.R. § 824.6(b), UC shall pay the civil penalty of $3,000,000 by check, draft, or money order payable to the Treasurer of the United States (Account 891099) mailed to the Director, Office of Enforcement, Attention: Office of the Docketing Clerk, at the above address. If UC fails to pay the civil penalties within the time specified and has not otherwise denied the violations or asserted that the penalties should be eliminated or reduced, the University will be issued an order imposing the civil penalty.

William C. Ostendorff
Acting Administrator
National Nuclear Security Administration

Washington, D.C.
This 13th day of July 2007

Enforcement Conference Summary

An enforcement conference was held with the University of California (UC) on April 13, 2007. Its purpose was to discuss potential violations of classified information security requirements identified in an Office of Enforcement Investigation Summary Report of April 2, 2007, concerning the unauthorized reproduction and removal of classified matter from Los Alamos National Laboratory (LANL) that was discovered in October 2006. Key points from the enforcement conference are summarized below.

Mr. Anthony Weadock, the designated DOE presiding officer for the enforcement conference, opened the conference and explained its purpose as providing a forum for UC to address the factual accuracy of DOE's Investigation Summary Report; address any of the facts or circumstances described in the report; provide UC input on any of the mitigation factors identified in DOE's General Statement of Enforcement Policy in 10 C.F.R. Part 824, Appendix A; and describe corrective actions being taken to address the issues disclosed by this incident.

UC's presentation of information was opened by Mr. S. Robert Foley, Jr., UC's Vice President for Laboratory Management. Mr. Foley indicated that UC takes the security incident seriously; however, it had not had much time to review the DOE Investigation Summary Report. Further, he pointed out that UC was not the contractor responsible for managing and operating the laboratory at the time of the incident, and he was unaware of any UC employees who were interviewed during the Department's investigation. Consequently, he did not think that UC could address any factual accuracy issues associated with DOE's Investigation Summary Report. However, he related UC's success in reducing the amount of classified removable electronic media (CREM) in 2003 and in undertaking the Red Network expansion project supporting the media-less computing environment. Mr. Robert Kuckuck, former Director of LANL, then spoke briefly, noting that budget shortfalls were significant during his tenure as the last UC Director of LANL and that UC's primary focus was on timely implementation of the Design Basis Threat by the end of 2006.

Mr. Terry Owens, UC Manager for Safeguards and Security, then provided information on several factors that UC believed DOE should consider toward mitigation in any enforcement action. These factors included: UC and DOE reliance on complementary systems to protect classified information; the subcontract worker involved in this security incident was well-trained to protect and handle classified information; DOE granted a "Q" clearance to the subcontract worker involved in the security incident; UC received good ratings for information security training; LANL policy made workers responsible for implementing all security requirements that apply to work performed; UC employed communication tools to impart security guidance; UC took actions to prevent security incidents and strengthen CREM accountability, including the development of laboratory policy to implement a single CREM accountability system; UC used

expert advisors, such as the Blue Ribbon Security Review Panel, to develop engineered tools for strengthened formality of operations; and expanded the media-less environment (Red Network Expansion Project).

UC noted that the Red Network expansion represented the best solution to prevent transfer of classified information to unclassified computers; and cited the laudatory review for implementation of Integrated Safeguards and Security Management (ISSM) and reduction of Laboratory Implementing Requirements. UC noted also that ISSM implementation provided workers with guidance, training, and tools to operate more securely and that UC management continued to improve ISSM implementation through the last day of UC's management contract (May 31, 2006); the FY 2005 receipt of a "good" rating in management, reflecting improvement; in FY 2006 – with few exceptions – rated "effective." This rating included an "outstanding" rating in response to program execution guidance provided by National Nuclear Security Administration (NNSA) security. The university asserted that increased risk was accepted in the face of budget reductions that resulted in the loss of a causal analysis tool (ESTHER) and the Help Desk, and the conduct of only half of the Classified Matter Protection and Control Self-Assessments. Finally, the DOE 470.1 series of directives could not be implemented. UC noted that increased security risks due to budget reductions were accepted by NNSA and, because of budget and transition issues, LASO agreed to delay full 470 implementation until FY 2007. Mr. Kuckuck reiterated that UC was constrained by budget and that employees were anxious and distracted during the contract transition period.

Mr. Foley then provided closing comments and a summary, in brief reiterating that UC takes this incident very seriously. He noted, however, that UC is no longer managing LANL, and the university did not investigate this incident.

When asked by Mr. Weadock to tie UC issues to the event, Mr. Gibbs offered that ISSM was used, though not fully. He further offered that, in hindsight, lessons could be learned associated with the escorting policy implementation, the reduction in protective force patrols and weekly walkdowns of the vault-type room, and administrative vs. engineering controls (for example, the use of locks on the computer rack).

Following UC's response, Mr. Shearer stated that sufficient time was provided to UC to prepare for the enforcement conference; however, due to the unique aspects of this case, the Office of Enforcement decided to permit UC to submit further information as it deemed appropriate. UC was informed that such information should focus on the facts and circumstances of the classified information security controls that were established during its tenure. Mr. Shearer advised that the Office of Enforcement would accept for consideration information that was received by April 30, 2007. Mr. Weadock thanked UC for the information provided, informed UC that a decision on any initiation of enforcement action would be provided in subsequent correspondence, and closed the enforcement conference.

On April 30, 2007, UC made an additional written submission. In summary, four main points were identified: 1) "UC takes the security incident seriously and believes that the DOE's Inspector General's determination that the root cause of the [subcontractor employee] having intentionally violated the regulations should be pursued vigorously." 2) "UC had a strong suite

of security systems in place." 3) "UC obtained the equivalent of a waiver of implementation of 470.4-1 and -4." 4) "The 10 C.F.R. 824 violation was committed by a LANS [Los Alamos National Security, LLC] subcontractor employee." The April 30 submission included an assertion that the university is immune from enforcement action under the Eleventh Amendment to the Constitution.

Enforcement Conference Attendees

University of California
Unauthorized Reproduction and Removal of Classified Material
from Los Alamos National Laboratory

April 13, 2007

Office of Enforcement
C. Russell H. Shearer, Chief for Enforcement and Technical Matters
Arnold E. Guevara, Director
Martha Thompson, Acting Deputy Director
Howard M. Wilchins, Senior Litigator
Tony Weadock, Acting Director
Steven Crowe, Acting Director
Peter D. Rodrik, Senior Enforcement Specialist
Hank J. George, Technical Advisor

Office of Security Technology and Assistance
Larry Wilcher, Director, HS-80

National Nuclear Security Administration
Robert Brese, Director, Office of Program Evaluations
Paul Detwiler, Deputy General Counsel
Mike Thompson, Director, Office of Facilities Operations
Edward Blackwood, Enforcement Coordinator
Janelle Zamore, Engineer

Los Alamos Site Office
Dan Glenn, Site Office Manager

University of California
Robert S. Foley, Jr., Vice-President Laboratory Management
Buck Koonce, Deputy Associate Vice-President of Laboratory Operations
Bill Eklund, General Counsel
Terry Owen, Director of Safeguards and Security
Scott Gibbs, former CSO & ADSFO LANL
Robert Kuckuck, former Director of LANL (Retired)