



Department of Energy
National Nuclear Security Administration
Washington, DC 20585

July 13, 2007

OFFICE OF THE ADMINISTRATOR

CERTIFIED MAIL
RETURN RECEIPT REQUESTED

Dr. Michael Anastasio
Laboratory Director
Los Alamos National Laboratory
MS-A100
SM-30, Bikini Atoll Road
Los Alamos, NM 87545

EA-2007-01

Subject: Preliminary Notice of Violation

Dear Dr. Anastasio:

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 upon the investigation of the incident and evaluation of the evidence in this matter, including information presented by you and members of your staff during the enforcement conference on April 13, 2007, I am issuing the enclosed Preliminary Notice of Violation (PNOV) in accordance with 10 C.F.R. § 824.6. A summary of the enforcement conference is also enclosed.

As set forth in the PNOV, DOE's National Nuclear Security Administration finds deficiencies in the security controls implemented by Los Alamos National Security, LLC (LANS) were a central factor in the thumb drive security breach discovered in October 2006, and that LANS is responsible for the actions of the subcontractor employee who perpetrated that breach. The enclosed PNOV details LANS's security management deficiencies and the actions of the subcontractor employee that resulted in the violation of DOE classified information security requirements, and proposes assessment of a civil penalty of \$300,000.


This incident is particularly troubling because many of the violations cited in the PNOV are of the same nature as other performance deficiencies that have occurred at LANL in the areas of safety and security. These violations arose from failures in the implementation of classified information security requirements as well as from the actions of the subcontractor employee (for whom LANS is accountable), and created vulnerabilities that led to the potential loss of national security interests. The history of problems and violations concerning the protection of classified information at LANL are matters of deep concern to the Department. We expect dramatic improvements in



LANS's performance, and will not hesitate to employ all aspects of the Department's authority to ensure LANS complies with the information security and other requirements of its management contract.

Pursuant to 10 C.F.R. § 824.6(a)(4), LANS 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 penalties it imposes, constitutes a final order.

Sincerely,


William C. Ostendorff
Acting Administrator
National Nuclear Security Administration

Enclosures: Preliminary Notice of Violation, EA-2007-01
Enforcement Conference Summary, EA-2007-01

cc: Gerald Parsky, Los Alamos National Security, LLC
Charles McMillan, Los Alamos National Security, LLC
Paul Sowa, Los Alamos National Security, LLC
Alverton Elliott, Los Alamos National Security, LLC
Steve Porter, Los Alamos National Security, LLC

Preliminary Notice of Violation

Los Alamos National Security, LLC
Los Alamos National Laboratory

EA-2007-01

The Office of Enforcement in 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 of Los Alamos National Security, LLC (LANS) conducting a classified document scanning project at the Los Alamos National Laboratory (LANL). The investigation identified violations at LANL of the DOE classified information protection requirements contained in the DOE Manual 470.4 series, in 10 C.F.R. Part 1045, *Nuclear Classification and Declassification*, and in DEAR clause 952.204-2 SECURITY (SEP 1997), which requires that DOE contractors “agree[] to comply with all security regulations and requirements of DOE in effect on the date of award [of their contract].” The Department’s National Nuclear Security Administration (NNSA) has concluded that LANS is responsible for some of these violations.

Pursuant to section 234B of the Atomic Energy Act of 1954, as amended, and 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 for violations of DOE’s classified information security requirements. Section 824.4(a)(2) authorizes the Department to take enforcement action and impose civil penalties for violations of classified information protection requirements contained in 10 C.F.R. Part 1045, *Nuclear Classification and Declassification*. Section 824.4(a)(3) additionally 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.” DOE issued the 470.4 series of manuals to codify its classified information protection requirements. Although violations of the 470.4 series manuals were identified in association with and as contributing to the subject event, NNSA in its discretion has determined no civil penalties will be assessed regarding requirements in this series of manuals.

Summary of Violations

In summary, NNSA finds that LANS 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 LANS on April 3, 2007.

- Violation of Requirement to Protect Data Ports - LANS failed to implement effective measures to correct a known vulnerability of unauthorized access to and downloading of classified information from LANL’s classified information systems. (See Violations, Section I.)
- Violation of Escorting Requirements - LANS did not impose adequate escorting controls of the employee of a LANS subcontractor at all times in order to prevent, detect, or deter the unauthorized access to and removal of electronic and documentary classified information to an unsecured site, namely, a private residence. (See Violations, Section II.)
- Violation of Physical Security Requirements - LANS 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, detect, or deter unauthorized removal of classified matter. (See Violations, Section III.)
- Violation of Requirements regarding Roles and Responsibilities – LANS failed to establish well defined roles and responsibilities for LANS security and line management personnel and the involvement of multiple organizations in the scanning project that led to confusion about roles. (See Violations, Section IV.)
- Violation of Requirements for Oversight of Subcontractors – LANS’s oversight of subcontractor activities was deficient in ensuring effective flowdown of and compliance with security requirements. (See Violations, Section V.)
- Violation of Requirements for Self-Assessment - LANS self-assessment processes were not effective in identifying the broad classified information security deficiencies disclosed by this incident. (See Violations, Section VI.)
- Violations Related to the Incident - The subcontractor employee performed unauthorized reproduction of numerous classified documents on paper and on removable electronic media, and took the copies from the site without authorization to a private residence, resulting in multiple violations by LANS in the following areas (see Violations, Section VII):
 1. Unauthorized reproduction of classified matter and generation of classified removable electronic media (CREM), including improper marking of the CREM;
 2. Unauthorized removal of classified matter and CREM from the site; and
 3. Unauthorized storage of classified matter and CREM in a private residence.

Violations

I. Violation of Requirements 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 “[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, at ¶ 2.c.(3)(e).

Contrary to this requirement, LANS failed to correct known vulnerabilities to prevent unauthorized access to and downloading of classified information in LANL’s cyber system. LANS 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) drive, or “thumb drive.” Similar vulnerabilities were noted in 1999, when a series of significant incidents of security concern resulted in a stand-down of operations at three weapons laboratories, including LANL. LANL and the management 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 LANL 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 inspection by the Office of Independent Oversight 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 a part of this corrective action, LANL also adopted an initiative to eliminate as many data ports as possible by replacing stand-alone computer systems and networks with a 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 in place under LANS through September 2006. In summary, uncontrolled data ports on classified computer systems were a known vulnerability under the University of California’s management of LANL and remained a vulnerability under LANS. By leaving USB ports unsecured in the VTR where the security incident occurred, LANS failed to ensure compliance with the established policy in this area and failed to adequately address a known vulnerability.
- B. To prevent unauthorized physical access to classified systems, locks were present on the computer rack cage in the subject VTR; however, the rack was not locked. Even with known

vulnerabilities involving unprotected ports, LANS did not ensure adequate physical security control.

- C. The subcontractor employee was able to introduce a personal thumb drive into the VTR and use it to download and remove from the site numerous classified documents. Interviews during DOE's investigation showed that at the time of the incident, the introduction of such personal media was not unusual, and was not prohibited in practice. Additionally, LANS had no process in place for evaluating the impact of new technologies on security risks from insiders. New devices, such as USB or firewire ports or thumb drives, were not comprehensively evaluated for their impact on security. Thus, effective security controls were not implemented to prevent the introduction into classified areas of these devices, which could allow unauthorized access to or loss of classified matter and its unauthorized removal.

These deficiencies in the protection of data ports constitute 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 original 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).

Contrary to these requirements, LANS 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. LANS violated these requirements as follows:

- A. The subcontractor employee was required to be escorted while working in the VTR on the scanning project. 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.

¹ Section V of Appendix A of 10 C.F.R. Part 824, *General Statement of Enforcement Policy*, 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.”

- B. Although the predecessor management and operating (M&O) contractor² made the determination that the scanning project should use continuous controls for this subcontractor employee over a period of more than one year, LANS did not question this arrangement when it assumed management responsibility of LANL, nor did LANS evaluate the substantial potential for security vulnerabilities when relying on continual escort controls over a long period of time.
- C. The subcontractor employee was given a work station that was not directly visible from the locations where certain escorts normally sat and performed their other work functions. Consequently, the escorts could not continually maintain visual control of the 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 because the escorts could not hear if the employee used the printer; printing documents was not part of the scanning project.
- E. Finally, the subcontractor employee was able to perform multiple unauthorized tasks, demonstrating that the escort function was not effective. The employee performed unauthorized printing of portions of hundreds of classified documents, inserted a thumb drive in the work station storage device supporting the scanning project, and performed one or more unauthorized downloads of hundreds of classified documents, all while supposedly under the control of an escort.

These deficient escort controls for the scanning project 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.” *Id.* at ¶ 4.c. In addition, DOE Manual 470.4-4, *Information Security* (Aug. 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).

² The prior M&O contractor, the University of California, is a member of LANS and therefore the university's institutional knowledge about this and other projects was available to LANS.

Contrary to these requirements, LANS failed to perform effective physical searches and inspections to detect or deter matter being removed from the subject VTR or the associated limited area to ensure that classified matter was not removed. LANS violated these requirements as follows:

- A. The DOE investigation team determined that random physical searches were conducted but were limited in scope and did not effectively focus on the unauthorized removal of classified information. DOE's investigation found that before this incident, an average of only ten random searches or inspections of hand-carried items were conducted per day for the entire LANL site, using only two protective force patrols. The LANL site has approximately 12,000 employees with access authorizations and over 100 VTRs.
- B. The DOE investigation team determined that before this event, LANS had not established a specific physical search requirement for LANL that focused on classified areas.
- C. Finally, the subcontractor employee was able to remove a large quantity of classified documents on paper and CREM without detection. Thus, the physical security measures that LANS applied to prevent, detect or deter unauthorized removal of classified material from the subject VTR were not effective.

These deficient physical search measures 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." *Id.* at ¶ 2.c.(3)(e).

Contrary to these requirements, roles and responsibilities for security and oversight related to the scanning project were not adequately delineated or implemented to ensure that security controls would function effectively to prevent, detect, or deter unauthorized access to and removal of classified matter. LANS violated these requirements as follows:

- A. With respect to line management of the project, the DOE investigation determined that the large number of LANL program organizations involved in the scanning project created confusion about who was responsible for project management and security roles. The subsequent LANS causal analysis of the event (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 occurred, the DOE investigation determined that 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.

These deficient delineations of roles and responsibilities constitute a Severity Level I violation.

V. Violation of Requirement 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.

Contrary to this requirement, LANS’s oversight of subcontractor activities was deficient and failed to ensure effective flowdown of and compliance with security requirements as follows:

- A. The extent of violations directly related to the incident as enumerated in Section VII demonstrates that LANS’s oversight activities were not effective in ensuring that the subcontractor employee complied with classified information protection requirements.
- B. The Core Team of the LANS Security Action Team (SAT) that was established immediately after the incident determined (*see Final Summary Report* (Dec. 15, 2006)) that responsibilities of the Contract Administrator (CA) and Subcontract Technical Representative (STR or TR) to ensure proper flowdown of and compliance with security requirements on the part of subcontractors and lower-tier subcontractors were neither clearly established nor understood.
- C. The SAT also determined that there was a lack of clarity and standardization in the security language used in subcontracts, and that very few STR and TR representatives understood the security requirements associated with their respective subcontracts.
- D. The SAT further determined that LANS subcontractors are neither aware of, nor are they flowing down to their employees and their lower-tier subcontractors, the applicable security requirements in accordance with their subcontracts or purchase orders.
- E. Finally, the SAT found that LANS lacks a robust oversight program to monitor subcontractor performance and implementation, including performance related to classified information protection.

These deficient controls in oversight of subcontractor security requirements and implementation constitute a Severity Level I violation.

VI. Violation of Requirements regarding Self-Assessment

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 “[c]ontractors must conduct self-assessments ... and include all applicable facility S&S program elements. The self-assessment must ensure the S&S objectives are met.” *Id.* at Attachment 2, Part 1, Section G, at ¶ 2.a.(6). This manual states that the objective of these self-assessments is to “[p]rovide assurance to the Secretary of Energy, Departmental elements, and other government agencies (OGAs) that safeguards and security (S&S) interests and activities are protected at the required levels.” *Id.* at ¶ 1.a.

Also, LANL’s *Contractor Assurance System, Security & Safeguards Self-Assessment Procedures* (June 16, 2006, and the prior version of Feb. 8, 2006) sets out the process for the planning and conduct of security self-assessments. That procedure states that the intent of the security self-assessments is “to identify and correct operational deficiencies.” *Id.* at ¶ 1.1.

In violation of these requirements, the LANS self-assessment process was ineffective in ensuring that security objectives were met and that security deficiencies were identified:

- A. The extent and number of violations and deficiencies in classified information protection revealed by this incident and by DOE investigations demonstrate that the LANS self-assessment process was not effective in discovering significant problems with classified information security.
- B. The DOE investigation team’s review of LANS’s rollup self-assessment reports of cyber security found that these assessments did not identify any substantive issues, and were conducted in a manner incapable of revealing the types of problems disclosed by the investigations and reviews following this security incident.
- C. DOE’s investigation determined that the annual cyber security threat assessments had historically focused on external threats. Although external threats pose a serious risk to the security of LANL classified information, the risk posed by internal threats was not adequately considered. In fact, the broader cyber security and classified information issues noted in DOE’s investigation pertain to risks from internal threats, as happened in this incident.

LANS’s deficient self-assessment process constitutes a Severity Level I violation.

VII. Violations Related to the Incident

Subsection a. of section 234B of the Atomic Energy Act authorizes DOE to take enforcement action and impose a civil penalty on “[a]ny person who has entered into a contract or agreement with the Department of Energy, or a subcontract or subagreement thereto, and who violates (or whose employee violates) any applicable rule, regulation, or order prescribed or otherwise issued by the Secretary pursuant to this Act relating to the safeguarding or security of Restricted Data or

other classified or sensitive information.” Section 1045.44 of title 10 of the Code of Federal Regulations requires that “[a]ny person with authorized access to RD [Restricted Data] or FRD [Formerly Restricted Data] who generates a document intended for public release in an RD or FRD subject area shall ensure that it is reviewed for classification by the appropriate DOE organization (for RD) or the appropriate DOE or DoD [Department of Defense] organization (for FRD) prior to its release.” 10 C.F.R. § 1045.44. Section 1045.40(a) of this title mandates that every document containing RD or FRD be clearly marked so as to convey its level of classification and that it contains RD or FRD. *Id.* at § 1045.40(a).

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, at ¶ 2.c.(3)(e). In addition, DOE Manual 470.4-4, *Information Security*, (Aug. 26, 2005) requires that:

1. Classified information must be protected and controlled.
2. Controls on classified information must prevent unauthorized access to it.
3. Security measures must prevent unauthorized visual and aural access.
4. Classified information must be disclosed only to individuals who have appropriate access authorization.
5. Classified matter must be maintained under the control of a person possessing the proper access authorization and need-to-know.
6. Removal of classified matter from approved facilities to private residences is prohibited.

Id. at ¶¶ 2.a, 2.d, 2.f, 2.g; Chapters II-2 & II-6.j.(4). This manual also requires that any matter originating and prepared in a classified area be reviewed for classification by a derivative classifier; that a classification review be performed before information is released outside the system boundary; that approval is obtained to hand-carry classified matter outside of a facility; that the cognizant security authority is notified whenever classified matter is hand-carried outside the facility; that a record of the classified matter be made before hand-carrying outside the facility; that, when not in use, classified matter must be stored only in DOE-approved facilities; and that a record of hand-carried accountable classified matter is maintained at the facility and with the individual transporting the matter. *Id.* at ¶¶ 1.c, 1.d, 6.j.(1), 6.j.(2), 6.j.(4)(a) & 6.j.(8).

The subcontractor employee violated these requirements when she performed unauthorized reproduction of classified documents on both paper and CREM and took the copies from the laboratory to a private residence. These actions by the employee constitute violations by LANS of each of the requirements regarding the protection of classified information cited above. These violations may be grouped as follows:

1. Unauthorized reproduction of classified matter and generation of CREM.
2. Unauthorized removal of classified matter and CREM from the site.
3. Improper marking of classified matter and unauthorized storage of CREM in a private residence.

These violations of 10 C.F.R. Part 1045 and DOE Manuals 470.4-1 and 470.4-4 constitute a Severity Level I violation.

VIII. Assessment of Civil Penalties

The violations set out above fall into two categories. Violations I through VI arise from the failures of LANS (and its predecessor, the University of California) to design and implement adequate procedures to protect classified information. Violation VII involves the willful disregard of security requirements by a single individual. As to the first category of violations, NNSA elects to forego the assessment of civil penalties. As to the second category, NNSA proposes to impose a penalty of \$300,000 against LANS for violation VII.

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.³ 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.⁴ 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;
 - Four documents (eleven pages) were Confidential/National Security Information (C/NSI); and
 - Thirty-two documents (sixty-five pages) were Unclassified.

³ 10 C.F.R. Part 824, Appendix A, ¶ V.a.

⁴ See footnote 1 *supra*.

- 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 the University of California’s tenure as LANL’s management contractor – that failed to correct 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. The report (at 17-18 and 25-29) discusses how this inadequate control system allowed the subcontractor employee to surreptitiously copy and remove classified matter from the laboratory. Based on the extensive inadequacies in the management-control system, the nature and amount of the classified material removed, the culpability of the subcontractor employee, and the duration of the violations, NNSA has concluded that each of the seven violations constitutes a Security Level I violation, the highest category of violation.

B. Potential Penalties

NNSA can impose penalties of up to \$100,000 for each day of each Security Level I violation. As to violations I-VI, they continued from June 1, 2006, the day LANS assumed responsibility for managing the laboratory, through at least October 17, 2006, the day the Los Alamos Police Department secured the materials discovered in a private residence. Accordingly, the maximum potential penalty for these violations is at least \$ 83.4 million (six violations x 139 days x \$100,000 per violation per day). As to violation VII, the Investigation Summary Report (at 26) finds that this violation continued for at least 48 days, while some aspects of it existed for a longer period of time. The maximum penalty for this violation is at least \$ 4.8 million.⁵

⁵ Section 234B.d.(2) of the Atomic Energy Act limits penalties to the amount of fee awarded to the contractor for the fiscal year in which the violations occurred. 42 U.S.C. § 2282b(d)(2). These violations began in fiscal year (FY) 2006 and continued into FY 2007. LANS received \$17.8 million in fee for FY 2006; it can receive up to \$73 million for FY 2007. Therefore, NNSA can impose at least \$17.8 million in fines for this incident, and perhaps more depending on the fee award for FY 2007.

C. Mitigation of Penalties

1. Violations I through VI

These violations arise from the deficient procedures established by the University of California for the scanning project (Violations I-V); or from LANS's inadequate self-assessment processes (Violation VI), which failed to identify and appreciate the weaknesses in the security procedures it had inherited from the university. Prior to LANS's assumption of responsibility for the management of LANL, the university had managed the laboratory for more than 60 years. One of the factors that led to the Department's decision to compete the contract for management of the laboratory was its troubling history of safety, security and operational problems. The mission of the laboratory is complex and critical to the nation, much of its work involves sensitive information and activities, and the laboratory's facilities are numerous and in many cases old. Both NNSA and LANS realized that the transition at LANL would be demanding, and that it would take time to address some of the problems that had led to the decision to compete the contract.

Once the severity of the thumb drive incident became clear to LANS, it accepted responsibility for the security breach and took steps to identify the deficiencies that had allowed this incident to occur.⁶ At the same time, it began to implement corrective actions that could be put in place quickly while it developed a plan that would focus on comprehensive steps for improving the protection of classified material over the long term. LANS also took actions to hold the subcontractor for the scanning project and the laboratory employees responsible for the project's security accountable for the incident.⁷ In light of these and other steps taken by LANS to address the deficiencies in its systems and processes for the protection of classified material, its acceptance of responsibility for the incident, and the challenges presented by the transition to a new contractor at LANL, NNSA has determined that it should not propose civil penalties for these violations. An additional factor in NNSA's decision not to impose penalties as to these six violations is that LANS will be subject to a Compliance Order issued by the Secretary of Energy. The order requires it to take specific steps to address the culture, procedures, and conditions that were the root cause of these violations. This order subjects LANS to severe monetary penalties if it fails to address these issues according to the schedule set forth in the order. The order, and the risk of penalties it poses for failing to comply with it, provide appropriate deterrence against future violations and incentive for implementing systems and procedures to better protect classified material.⁸

⁶ LANS's initial notifications to the Department concerning this incident were not as prompt as they should have been. NNSA expects LANS to evaluate its shortcomings in this regard and learn from them.

⁷ LANS described its responses to this incident at the enforcement conference on April 13, 2007. A summary of the conference is attached. At the conference, LANS provided the Department with a document that contained additional details about its responses. *Unauthorized Reproduction and Removal of Classified Material – 10 C.F.R. Enforcement Conference* (Apr. 13, 2007).

⁸ LANS asserted that the Department could not impose civil penalties for these six violations because, at the time of the incident, its contract cited DOE manuals that did not provide that violations of requirements in these manuals

2. Violation VII

This violation arises from the subcontractor employee's willful violation of numerous security requirements. The maximum potential penalty for this violation is at least \$4.8 million, as the violation continued for at least 48 days. Many of the mitigating factors that informed NNSA's decision on penalties for the first six violations are also relevant here. The subcontractor employee's actions occurred soon after the transition. If the prior contractor had implemented security procedures for the scanning project that complied with DOE's requirements, the employee might have been deterred or prevented from removing the classified matter. However, LANS is in error in asserting that it should not be held responsible for the willful actions of an employee of one of its subcontractors. Both LANS and the University of California observed erratic behavior by the employee that should have caused them to question her reliability for this project.⁹ As noted in DOE's General Statement of Enforcement Policy:

[A] violation may be deemed to be more significant if a senior manager of an organization is involved rather than a foreman or a non-supervisory employee. In this regard, while management involvement, direct or indirect, in a violation may lead to an increase in the severity level of a violation and proposed civil penalty, *the lack of such involvement will not constitute grounds to reduce the severity level of a 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.*

10 C.F.R. Part 824, Appendix A, ¶ V(d)(emphasis added); *see also* 42 U.S.C. § 2282b(a) & Part 824, Appendix A, ¶ VIII(1)(d) (“contractors normally will be held responsible for the acts or omissions of their employees and subcontractor employees in the conduct of activities at DOE facilities”). Vigilance is a critical defense against the threats posed to classified information by opportunistic and malicious insiders. LANS ignored signs concerning the reliability of this employee that, had they been heeded, might have prevented this incident or limited its scope.

In light of these considerations, NNSA proposes to reduce the civil penalty for this violation from \$4.8 million to \$300,000.

could result in civil penalties. *Id.* at 64-65; *see also* 10 C.F.R. § 824.4(a)(3). Because NNSA has decided not to impose any penalties as to these violations, that question is moot.


⁹ *See, e.g., Unauthorized Reproduction and Removal of Classified Material* at 62.

Opportunity to Respond

Pursuant to the provisions of 10 C.F.R. § 824.6, LANS may submit a written reply to this PNOV within 30 calendar days of its receipt. 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 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 been provided already. If no reply is submitted within 30 calendar days, in accordance with 10 C.F.R. § 824.6(c), this preliminary notice of violation, including the proposed penalties, constitutes a final order.

Within 30 calendar days after receipt of this PNOV, unless LANS denies the violations or asserts that the penalties should not be imposed or should be reduced, LANS shall pay the civil penalty of \$300,000 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 LANS 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, LANS will be issued an order imposing the civil penalty.


William C. Ostendorf
Acting Administrator
National Nuclear Security
Administration

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

ENFORCEMENT CONFERENCE SUMMARY

An enforcement conference was held with Los Alamos National Security, LLC (LANS) 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 issued on April 2, 2007, associated with the unauthorized reproduction and removal of classified matter from Los Alamos National Laboratory (LANL) that was discovered in October 2006. Selected topics 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 LANS to address the factual accuracy of DOE's Investigation Summary Report; address any of the facts or circumstances described in the report; provide LANS's input on any of the mitigation factors identified in DOE's Enforcement Policy in Appendix A of Part 824; and describe corrective actions being taken to address the issues disclosed by this incident.

LANS's presentation was introduced by Dr. Michael Anastasio, President of LANS and Laboratory Director of LANL. Dr. Anastasio indicated that LANS had no issues with the factual accuracy of DOE's Investigation Summary Report. He described LANS's acceptance of ownership of the problems disclosed by the incident and of the solutions to these problems. He went on to summarize the steps that LANS had taken as part of its due diligence before assuming management of LANL, and provided an overview of the immediate actions taken not only in the classified vault-type room in question but for the broader issues that were revealed by the incident. Mr. Paul Sowa then described the immediate security actions that were taken, the cooperative working relationship between LANS and the Federal Bureau of Investigation (FBI) to aid the FBI investigation, formation of a LANL Security Action Team, conduct of a LANS Security Incident Team Inquiry, and longer-term steps to improve protection of classified information and cyber security.

Mr. Charles McMillan then described the causal analysis that was performed, the methodology used, and the conclusions reached. The results pointed to further systemic issues needing attention, many falling under the umbrella of greater rigor in implementation of integrated safeguards and security management (ISSM).

Mr. Roger Hagenruber then described the corrective steps that were being taken to more deeply embed ISSM in the LANL workforce, assess and improve the organizational culture and attitude, and institute a more comprehensive human performance improvement program with respect to classified information protection. Mr. Hagenruber then described the changes being made to establish a centralized cyber security function focused on achieving compliance with cyber security requirements, minimizing vulnerabilities in the current operating environment, and creating a longer-term cyber security environment that is inherently more secure. He further described a cyber security integrated project team that was evaluating issues from past assessments and lessons learned from recent events, integrating these with findings from the

most recent event's causal analysis, and developing a comprehensive corrective action plan for cyber security.

Steve Porter, LANS General Counsel, provided information on several factors that LANS believed should be considered by DOE toward mitigation in any enforcement action. One of the matters raised by Mr. Porter was whether LANS could be held liable for the willful act of a subcontractor employee. Mr. Porter also argued that DOE should exercise its enforcement discretion in this matter because the conditions allowing the event to occur were latent and because LANS only recently became the contractor at LANL and thus had not had an opportunity to uncover and correct deficiencies.

Dr. Anastasio then provided closing comments and a summary, indicating that LANS takes this incident very seriously, took immediate actions to address the deficiencies, is accelerating plans for a more robust security system, and is implementing an integrated approach to security.

Following LANS's response to a number of questions from DOE officials, Mr. Weadock thanked LANS for the information provided, informed LANS that the Department would provide its determinations in subsequent correspondence, and closed the conference.

ENFORCEMENT CONFERENCE ATTENDEES

Los Alamos National Security, L.L.C.
Unauthorized Reproduction and Removal of Classified Material
from Los Alamos National Laboratory

April 13, 2007

Office of Health, Safety and Security

C. Russell H. Shearer, Deputy Chief for Enforcement and Technical Matters (HS-1)
Arnold E. Guevara, Director, HS-40
Martha S. Thompson, Acting Deputy Director, HS-40
Howard M. Wilchins, Senior Litigator, HS-40
Steven G. Crowe, Acting Director, HS-43
Tony Weadock, Senior Enforcement Specialist, HS-42
Peter D. Rodrik, Senior Enforcement Specialist, HS-42
Larry Wilcher, Director, HS-80
Hank George, Technical Advisor

National Nuclear Security Administration

Robert Brese, Director, NA-74
Paul Detwiler, Deputy General Counsel, NA-3.1
Mike Thompson, Technical Director, NA-171
Edward Blackwood, PAAA Coordinator, NA-3.6

Los Alamos Site Office

Dan Glenn, Manager

Los Alamos National Security, L.L.C.

Michael Anastasio, Laboratory Director
Rich Marquez, Executive Director
Charles McMillan, Associate Director, Weapons Physics
Paul Sowa, Associate Director, Security and Safeguards
Roger Hagenruber, Chief Security Officer
Steven Porter, General Counsel
Pablo Prando, General Counsel
Al Elliott, PAAA Coordinator
Matt Hardy, Advisor
David Lyons, Office Leader