The Secretary of Energy
Washington, DC 20585

July 12, 2007

CERTIFIED MAIL
RETURN RECEIPT REQUESTED

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

Dear Dr. Anastasio:

Pursuant to the authority of the Secretary of Energy under section 234B of the Atomic Energy Act of 1954, as amended, and 10 C.F.R. § 824.4(b) of the Department's *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, I am today issuing the enclosed Compliance Order to Los Alamos National Security, LLC (LANS).

The Compliance Order directs LANS to implement specific corrective actions to remediate both the laboratory management deficiencies that contributed to the thumb drive security incident at Los Alamos National Laboratory (LANL) discovered in October 2006 and, more broadly, longstanding deficiencies in the classified information and cyber security programs at LANL.

Violation of the Compliance Order would subject LANS to issuance of a notice of violation and assessment of civil penalties up to $100,000 per violation per day. Pursuant to 10 C.F.R. § 824.4(b), if LANS wishes to contest the Compliance Order, it must file a notice of appeal within 15 days of receipt of the Compliance Order.

Sincerely,

Sam Bodman

Samuel W. Bodman

Enclosure

cc: Gerald Parsky, Los Alamos National Security, LLC
Charles McMillian, Los Alamos National Security, LLC
Paul Sowa, Los Alamos National Security, LLC
Alverton Elliott, Los Alamos National Security, LLC

Printed on recycled paper

UNITED STATES
DEPARTMENT OF ENERGY

In The Matter Of	)	EA-2007-01
Los Alamos National Security, LLC	)	
Los Alamos National Laboratory	)	
Los Alamos, New Mexico	)	

COMPLIANCE ORDER REQUIRING CLASSIFIED INFORMATION SECURITY CORRECTIVE MEASURES (EFFECTIVE JULY 12, 2007)

This Compliance Order, issued pursuant to 10 C.F.R. § 824.4(b), directs Los Alamos National Security, LLC, (hereinafter "LANS") to implement the corrective measures set forth in Section IV hereof in order to remedy deficiencies in LANS information and cyber security programs.

I

LANS is the management and operating contractor for LANL in New Mexico. Since June 1, 2006, LANS has managed and operated LANL under Contract No. DE-AC52-06NA25369 ("Contract") for the Department of Energy's National Nuclear Security Administration (NNSA), and the Department requires that LANS ensure the protection of national security interests, including classified information at LANL, in accordance with DOE requirements set forth in the Contract. This Order directs LANS to take specific remedial actions to correct deficiencies in implementation of classified information protection and cyber security programs.

II

In October 2006, classified documents on removable electronic media and paper were discovered by the Los Alamos Police Department in the residence of a former employee of a LANL subcontractor. Multiple investigations (Office of Inspector General and DOE) determined that the documents had been removed from LANL by the employee while she had been performing work in support of a classified document scanning project in one of LANL's vault-type rooms (VTRs). Some of the documents were classified as Secret and contained critical national security interest information.

DOE's investigation into this incident (Investigation Summary Report, dated April 2, 2007 entitled, "Unauthorized Reproduction and Removal of Classified Matter from Los Alamos National Laboratory"), hereinafter referred to as "the security incident," as well as

subsequent inquiries and evaluations by LANS, identified numerous breakdowns in LANL's classified information protection and cyber security program, not only as to the breakdowns that resulted in the incident itself but also in the LANL programs that LANS and DOE rely on to protect classified information and to prevent such incidents. DOE has concluded that these breakdowns were caused by poor security practices, a weak cyber security program, and a lack of management attention to the classified scanning project activities within the VTR, and that proper management attention could have prevented the incident.

Subsequent to this incident and LANS's inquiry into it, LANS conducted a causal analysis and concluded that the direct cause was the employee's deliberate violation of at least 11 security requirements and controls intended to protect classified matter stored in the VTR. It concluded that the root cause was that LANL has not consistently and effectively implemented the guiding principles and core functions of Integrated Safeguards and Security Management (ISSM) in the management of its classified work.

This security incident is another in a series of serious classified information and cyber security incidents at LANL over the last decade. Although some corrective steps were taken by the previous LANL contractor, the University of California, in response to these prior incidents, the security incident uncovered in October 2006 demonstrates that problems in these areas have continued under LANS's tenure as the management contractor at LANL.

In addition to problems in classified information and cyber security revealed by these incidents, a number of deficiencies in these areas were identified by various DOE assessments and are listed in the Department's Safeguards and Security Information Management System (SSIMS).

Accordingly, this Compliance Order directs LANS to undertake comprehensive steps to ensure that critical classified information and cyber security deficiencies at LANL are identified and addressed.

III

LANS must undertake a comprehensive review of the deficiencies in its classified information security and cyber security programs, including those revealed by this incident, those discovered in previous security incidents, and those identified during various assessments of LANL (for example, self-assessments, Field Element Security Survey Reports, Independent Oversight Inspection Reports, Office of Inspector General and Government Accountability Office reports). LANS must make a rigorous and comprehensive evaluation of the underlying causes of continuing security problems, in the context of the findings of these other assessments, in order to develop an integrated and effective long-term solution. LANS is required to submit (1) the results of this review and (2) an Integrated Corrective Action Plan to NNSA – Los Alamos Site Office (LASO) for

approval in order to ensure that the Department, including the National Nuclear Security Administration, not only assists but also provides the critical oversight LANS needs to achieve success.

LANS is also required immediately to take steps to improve the LANL organizational culture in terms of attitudes, behaviors, and practices regarding classified information and cyber security. It is imperative that LANS management demonstrate leadership in this area so that workers, researchers and supervisors work together to assure that rigorous attention is given to security requirements, a proper questioning attitude is displayed, conservative assumptions and decisions are applied, and issues and concerns are openly communicated. This Compliance Order also directs LANS to extend its issues management process to resolution of safeguards and security issues including cyber security. It is expected that this process will result in a timely and effective resolution of the issues noted herein, as well as those that may be identified in the future using a structured management process.

In addition, LANS is directed to undertake a rapid review of compliance with and implementation of DOE-NNSA and Director of Central Intelligence cyber security directives,[1] completion of the new initial "Super VTR," and upgrades of security for all VTRs. The "Super VTR," which is to include classified work areas, media storage units, servers, and CREM[2] storage, is intended to allow consolidation of classified holdings and implementation of uniform controls for classified information while facilitating access for authorized users. Once LASO approves the operation of the "Super VTR" and classified assets are consolidated in it, the number of VTRs and accountable-CREM libraries at LANL can be reduced.

This Order also directs LANS to conduct independent assessments to confirm that the actions identified in Section IV have been completed as required by the Order, and that the completed actions are effective in resolving identified problems in classified information protection and cyber security. Finally, LANS is directed to provide quarterly briefings to DOE and NNSA officials on progress in completing actions, as well as demonstrating performance in these areas.

---

[1] For example, DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, DOE M 470.4-2 *Physical Protection*, DOE M 470.4-4, *Information Security*, NNSA Policy Letters (NAP) 14.1B and 14.2B, Director Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*, DOE O 5639.8A, *Security of Foreign Intelligence Information and Sensitive Compartmented Information Facilities*, DOE O 5670.1A, *Management and Control of Foreign Intelligence*.

[2] Classified Removable Electronic Media.

IV

Accordingly, pursuant to section 234B of the Atomic Energy Act of 1954, as amended, and 10 C.F.R. § 824.4(b), IT IS HEREBY ORDERED THAT

Classified Information and Cyber Security Management

1. *IMMEDIATELY* – LANS shall undertake measures to address organizational culture issues such as lack of classified information protection ownership by all employees, lack of leadership in classified information protection by LANL management, and failure to comprehensively implement Integrated Safeguards and Security Management (ISSM). LANS shall incorporate any such immediate measures as well as longer term actions to address these issues in the Integrated Corrective Action Plan required by corrective action 5 below.

2. *WITHIN 30 DAYS* – LANS shall perform an analysis of all LANL classified information and cyber security deficiencies reported to the Department's Safeguards and Security Information Management System (SSIMS) from 1999 to the date of this Compliance Order. The analysis shall be directed at identifying trends, recurring issues, and related systemic deficiencies in the areas of classified information and cyber security. The SSIMS analysis results should be incorporated into the review required by corrective action 3 below.

3. *WITHIN 30 DAYS* – LANS shall perform a comprehensive review to ensure that all classified information and cyber security issues at LANL are identified. The review shall address, but not be limited to, the following issues:

   a. Issues disclosed by the October 2006 security incident and follow-up reviews (including the Security Action Team review, the corporate review of cyber security, and the LANS inquiry into the event).

   b. Underlying causes, as identified in the LANS causal analysis, of the security incident. These should include (but not be limited to) the failure to effectively implement ISSM; the reliance on administrative rather than engineered security controls; and the lack of effective policies and controls for evaluating the risks associated with emerging cyber technologies.

   c. Input from the SSIMS analysis as described in corrective action 2 above.

   d. Any additional issues that LANS concludes contributed to the classified information and cyber security incidents at LANL since 1999.

   The LANS report of this comprehensive review shall be submitted to NNSA-LASO for approval, with resolution of any issues identified by NNSA-LASO,

WITHIN 45 DAYS of this Order. The LANS report of this review for classified intelligence information and deficiencies shall be submitted to the DOE Office of Intelligence and Counterintelligence (IN) for approval, with resolution of any issues identified by IN, within 45 DAYS of this Order.

4. *WITHIN 45 DAYS* – LANS shall submit an implementation plan to enhance its issues management process to more effectively implement resolution of physical and cyber security deficiencies. This plan shall ensure that physical and cyber security deficiencies are resolved in a timely manner, appropriate causal determinations are performed, corrective actions are taken to prevent recurrence, appropriate trending analysis of issues is used to identify recurring or programmatic issues, and performance indicators of deficiency resolution and trending are provided for management review. This plan shall be subject to approval by NNSA-LASO.

5. *WITHIN 60 DAYS* – LANS shall develop an Integrated Corrective Action Plan for those critical issues identified as a result of corrective action 3 above. The plan shall include those actions that have already been completed by LANS or are underway if they are considered to be part of the solution of the issues as a result of corrective action 3 above. The plan shall specifically include those actions established by LANS to develop, deploy, and sustain a more effective ISSM process and culture at the laboratory. This plan shall be submitted to NNSA-LASO for approval, and actions shall be placed in DOE's SSIMS.

Additional Specific Cyber Security Actions

6. *BY AUGUST 17, 2007* – LANS shall complete a Laboratory-Wide Cyber Security Self Assessment of conformance with National Institute for Standards and Technology (NIST) 800-53A and Director of Central Intelligence Directives (DCID). *WITHIN 30 DAYS* of that date, LANS shall resolve any NNSA-LASO and IN concerns and obtain NNSA-LASO and IN approvals as appropriate.

7. *BY AUGUST 30, 2007* – LANS shall develop and publish a comprehensive policy for compliance with all current cyber security requirements applicable to LANL. *WITHIN 30 DAYS* of that date, LANS shall resolve any NNSA-LASO and IN concerns and obtain NNSA-LASO approvals as appropriate.

8. *BY MARCH 31, 2008* – LANS shall fully implement all NNSA Policy Letters (NAPs) concerning Cyber Security. *WITHIN 30 DAYS* of that date, LANS shall resolve any NNSA-LASO and IN concerns and obtain NNSA-LASO approvals as appropriate.

9. *BY SEPTEMBER 30, 2008* – LANS shall achieve accreditation of all unclassified LANL systems pursuant to NAP requirements. *BY DECEMBER 12, 2008*, LANS shall achieve re-accreditation of all classified LANL systems pursuant to NAP and DCID requirements as appropriate.

VTR Security

10. *BY AUGUST 1, 2007* – LANS shall develop and establish a viable and effective Vault Type Room/Complex (VTR/VTRC) Certification/Re-certification program approved by NNSA-LASO that incorporates all physical security requirements as defined by DOE Directives, including VTR entry and exit inspections of individuals and escorting of visitors in VTRs. Any deviations from physical security policy shall be transmitted to NNSA-LASO to obtain appropriate approvals, and entered into SSIMS.

11. *BY SEPTEMBER 28, 2007* – LANS shall have the NNSA-LASO-approved prototype Super VTR operational to process classified information.

Communication and Verification

12. *BY NOVEMBER 1, 2007* – LANS shall submit to NNSA-LASO a report of an assessment by individuals independent from LANL, confirming the completion of the above actions that were required to be completed by August 30, 2007, and the effectiveness of those actions. Additionally, *WITHIN 30 DAYS* of completion of the independent assessment, an action plan addressing any findings and observations of this independent assessment shall be submitted to NNSA-LASO for approval.

13. *BY FEBRUARY 12, 2008* – LANS shall submit directly to NNSA-LASO a report of an assessment by individuals independent from LANL, confirming the completion of the remaining actions and the effectiveness of those actions. Additionally, *WITHIN 30 DAYS* of completion of this independent assessment, an action plan addressing any findings and observations of this independent assessment shall be submitted to NNSA-LASO for approval.

14. At *QUARTERLY* intervals from the issuance of this Order, LANS shall provide status updates at meetings with NNSA Headquarters, LASO and the Office of Enforcement. These meetings shall continue until completion of all of actions listed above. LANS shall provide information demonstrating substantive progress on corrective actions in accordance with Plan schedules and improvement in classified information and cyber security performance.

V

This Order constitutes a Final Order of the Department of Energy and is effective upon issuance. LANS may, within 15 days of receipt of this Order, file a notice of appeal with the Secretary of Energy to rescind or modify the Order in accordance with 10 C.F.R. § 824.4(b). The request may identify any proposed changes to specific actions to resolve issues of appropriateness or reasonableness. Any such request to modify or rescind should be directed to the Secretary of Energy, U.S. Department of Energy, 1000 Independence

Avenue SW, Washington, D.C. 20585, and should state good cause for the request. Any request to modify or rescind does not stay the effectiveness of the Order unless the Secretary issues an order to that effect.

As set forth in 10 C.F.R. § 824.4(b), any violation of this Order subjects LANS to issuance of a notice of violation and assessment of civil penalties in accordance with section 234B of the Atomic Energy Act of 1954, as amended, and 10 C.F.R. Part 824, of up to $100,000 per day for each violation.

Samuel W. Bodman
Secretary of Energy

Washington, D.C.
This 12th day of July 2007