LLNL-TR-456661

LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

Level-2 Milestone 3508: Certify and Accredit Livermore Computing to NAPS 14.2C

Milestone Report for NNSA HQ

Prepared by Pam Hamilton
September 23, 2010

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

Contents

Contents i
Introduction 1
Livermore Computing Activities 1
Attachment 1: Milestone Definition Text 4
Attachment 2: Accreditation Letter 5
Attachment 3: IATT Letter 7

Introduction

This report documents Livermore Computing (LC) activities in support of certifying and accrediting LC's Secure Computing Facility's (SCF) NAPS 14.2c compliant Information System Security Plan (ISSP), ASC L2 milestone 3508: Certify and Accredit Livermore Computing to NAPS 14.2c, due September 30, 2010. The full text of the milestone is included in Attachment 1. The description of the milestone is:

> *LC's cyber security plan accreditation expires March 31, 2010. A new plan must be written to be compliant with the NNSA's NAPS 14.2c cyber security policy. This new policy requires a complete overhaul of LLNL's classified security plans. LC will be a major contributor in the effort to create a Site Security Component Library, which will be used as a basis for LC's NAPS compliant plan. All new security test and evaluation plans will be developed to demonstrate NAPS compliance. Ultimately, the LC Information System Security Plan (ISSP) will be developed and delivered. This milestone is complete when the ISSP and the security test and evaluation plans have been submitted and LC has received interim approval to test.*

The milestone was completed on August 20, 2010 when a letter from the NNSA Livermore Site Office (LSO) was received by Mr. John E. Lewis, Director of LLNL's Security Organization, granting LC SCF "Approval to Operate". The letter is included in Attachment 2. The accreditation as stated in the letter is effective until August 18, 2013.

Livermore Computing Activities

Livermore Computing's cyber security plan for SCF was set to expire March 31, 2010. A six month extension (to September 30, 2010), was granted to allow LLNL time to proceed with a site-wide NAPS implementation effort for both unclassified and classified computing.

The NAPS primarily consist of two NNSA policy letters: *NAP 14.1-C, NNSA Baseline Cyber Security Program*; and *NAP 14.2-C, NNSA C&A Process for Information Systems*. LLNL's NAPS implementation plan defined one set of requirements for both classified and unclassified computing. These new requirements included a centralization of classified systems security plans; a new security plan format; new System Test and Evaluation reports; minimum security configuration standards; and stronger risk assessments.

Livermore Computing was a key player in the development of minimum security configuration standards to meet the NAPS requirements. The framework for implementing these NAPS-compliant component configurations is the Site Security Component Library (SSCL). Each entry in the SSCL has an approved configuration, a security test script, and ensures NAP-compliance based on NIST, NSA, DISA, CIS and other national standards. LC contributed six SSCL entries for the following operating systems:

- AIX (IBM)
- CHAOS (Linux)
- CHAOS-viz (Linux visualization)
- Debian (Linux)
- SLES (Linux)
- Solaris (Oracle)

LC also developed an Information System Security Plan for the SCF computing environment. An ISSP provides information necessary to secure an information system throughout its life cycle. It consists of three major parts: the System Description; the System Component Implementation; and any Interconnect Agreements. Details of LC's environment are covered in the System Description and include descriptions for the following information system components:

- Network Switches/Fabrics
- Servers
    - High performance computers
    - Visualization
- Infrastructure Services
    - General purpose servers
    - Network backup
    - Resource management
    - Authentication and directory services
    - Network attached file systems
    - Off-site backup
    - Console gateway
    - Common tools
- Global Parallel File Systems
- Archival Data Storage

LC staff also participated in the development of the new NAP-compliant LLNL Security Plan Policy (SPP) and the template for the System Test and Evaluation reports. NAP 14.2c defines NNSA requirements and recommended controls for information systems. There are a total of 169 controls divided among three different classes: Management; Operational; and Technical. Each control must have an implementation of how the control is met. For every NAP control the SPP includes the following:

- Policy (the NAP text)
- Supplemental guidance
- Implementation
- Potential assessment methods
    - Examine, interview, test
    - NIST 800.53 measures

The System Test and Evaluation (ST&E) reports are derived from the SPP. There is an Institutional ST&E report, addressing 132 controls which can be answered once for the site or "institution". The remaining 37 controls are addressed in LC's local ST&E report.

LLNL's Cyber Security Program (CSP) submitted LC's initial SCF ISSP and ST&E report to LSO on February 26, 2010. After reviewing the initial package, LSO granted Interim Approval To Test (IATT) on March 31, 2010. Attachment 3 is a copy of LSO's letter granting IATT. CSP submitted the LC SCF ISSP and the LC ST&E in their final form, and other relevant documents to LSO on August 12, 2010, along with the request to grant accreditation and "Approval to Operate".

The milestone was completed on August 20, 2010, when a letter from LSO was received by Mr. John E. Lewis, Director of LLNL's Security Organization, granting LC SCF "Approval to Operate". The letter is included in Attachment 2. The accreditation as stated in the letter is effective until August 18, 2013.

Attachment 1: Milestone Definition Text

Milestone (ID#3508): Certify and Accredit Livermore Computing to NAPS 14.2c		
Level: 2	**Fiscal Year**: FY10	**DOE Area/Campaign**: ASC
Completion Date: September 30, 2010		
ASC nWBS Subprogram: FOUS		
Participating Sites: LLNL		
Participating Programs/Campaigns: ASC		
Description: LC's cyber security plan accreditation expires March 31, 2010. A new plan must be written to be compliant with the NNSA's NAPS 14.2c cyber security policy. This new policy requires a complete overhaul of LLNL's classified security plans. LC will be a major contributor in the effort to create a Site Security Component Library, which will be used as a basis for LC's NAPS compliant plan. All new security test and evaluation plans will be developed to demonstrate NAPS compliance. Ultimately, the LC Information System Security Plan (ISSP) will be developed and delivered. This milestone is complete when the ISSP and the security test and evaluation plans have been submitted and LC has received interim approval to test.		
Completion Criteria: This milestone is complete when the ISSP and the security test and evaluation plans have been submitted and LC has received interim approval to test.		
Customer: LLNL ASC Program		
Milestone Certification Method: A report will be prepared to document completion of this milestone. A memo will be supplied that documents the Livermore Site Office's approval for LC to execute its Security Test and Evaluation plans.		
Supporting Resources: Livermore Site Office, LLNL Computer Security Program, LLNL's iSRD Team		
Supporting Milestones:		

Program	**Title**	**Due Date**
N/A	N/A	N/A

Codes/Simulation Tools Employed: None
Contribution to the ASC Program: Approval of this plan is required to continue operating the LC, which contains all the ASC HPC resources.
Contribution to Stockpile Stewardship:

No.	**Risk Description**	**Risk Assessment (low, medium, high)**		
		Consequence	**Likelihood**	**Exposure**
1	Security Plan is not approved on time.	High	Medium	High

Attachment 2: Accreditation Letter

U. S. Department of Energy
National Nuclear Security Administration
Livermore Site Office
PO Box 808, L-293
7000 East Avenue
Livermore, California 94551-0808

AUG 2 0 2010

5632.2
COR-SS-8/13/2010-274929

Mr. John E. Lewis
Director
Security Organization
Lawrence Livermore National Security, LLC
Lawrence Livermore National Laboratory
7000 East Avenue, L-503
Livermore, CA 94550

Subject: Accreditation of the Secure Computing Facility Classified Information System

References: (1) SOM-LTR-10-006605 (J. Lewis/D. Gordon), *Certification and Request for Accreditation of the Livermore Computing Secure Computing Facility (LC SCF) Information System Security Plan, 6138-MU-L*, dated August 12, 2010

(2) CS10-109 (G. Blair/D. Thompson), *Certification and Request for Accreditation of the Livermore Computing Secure Computing Facility (LC SCF) Information System Security Plan, 6138-MU-L*, dated August 12, 2010

Dear Mr. Lewis:

The Livermore Site Office (LSO) reviewed your request for accreditation of the Lawrence Livermore National Laboratory (LLNL) Secure Computing Facility (SCF) classified information system. LSO accredits the SCF to process Secret Restricted Data. This decision was made on the basis of our review of the following documentation, submitted with references (1) and (2):

- *Information System Security Plan for Livermore Computing Secure Computing Facility, 6138-MU-L, v.1.0*, dated February 2010; and
- Security Test and Evaluation Reports and LLNL certification statement, dated August 12, 2010.

"Approval to Operate" the SCF classified information system is effective until August 18, 2013, or until security significant changes occur that require re-accreditation.

If you should have any questions, please contact Don Thompson at (925) 422-2248.

Sincerely,

Duane G. Gordon
Designated Approving Authority

cc:
D. Thompson
G. Blair
D. Crawford
E. Matsche

Attachment 3: IATT Letter

U. S. Department of Energy
National Nuclear Security Administration
Livermore Site Office
PO Box 808, L-293
7000 East Avenue
Livermore, California 94551-0808

RECEIVED
MAR 3 1 2010
2010 APR -6 A 8: 31
LLNL COMPUTER SECURITY

5637.2
COR-SS-2/24/2010-236614

Mr. John E. Lewis
Director
Security Organization
Lawrence Livermore National Security, LLC
Lawrence Livermore National Laboratory
7000 East Avenue, L-503
Livermore, CA 94550

Subject: Interim Approval to Test for System 6138-MU-L, *Secure Computing Facility*

References: (1) SOM-LTR-10-006103 (J. Lewis/D. Gordon), *Request for Interim Approval to Test for System 6138-MU-L, SCF*, dated February 23, 2010

(2) CS10-032 (G. Blair/D. Thompson), *Request for Interim Approval to Test for System 6138-MU-L, SCF*, dated February 23, 2010

(3) CS10-55 (G. Blair/D. Thompson), *Supplemental Information Regarding Information System Security Plan (ISSP) 6138-MU-L (SCF)*, dated March 26, 2010

Dear Mr. Lewis:

The Livermore Site Office (LSO) reviewed the subject request for Interim Approval to Test (IATT) the Lawrence Livermore National Laboratory (LLNL) Secure Computing Facility (SCF). In support of this request, LLNL submitted an Information System Security Plan (ISSP) that describes the National Nuclear Security Administration Policy (NAP) based cyber controls used for the protection of Secret Restricted Data. This ISSP is comprised of the following documents:

- *Information System Security Plan for Livermore Computing Secure Computing Facility, 6138-MU-L, V1.0*, dated February 2010, references (1) and (2);
- LLNL NAP 14.2-C, *LLNL Security Plan Policy (SPP) NAP14.2-C Security Controls, Version 1.5.1*, dated March 19, 2010; and
- System configuration information provided in reference (3).

LSO grants IATT the LLNL SCF. This approval is effective until September 30, 2010. During the IATT period, the SCF ISSP (*6138-MU-L, V1.0*, dated February 2010) is the governing Cyber Security Plan for this Information System.

If you should have any questions, please contact Don Thompson at (925) 422-2248.

Sincerely,

Duane G. Gordon
Designated Approving Authority

cc:
D. Thompson
G. Blair
D. Crawford
E. Matsche