Cyber Security Plan
for the
SC Lattice QCD Computing Project Extension II
(LQCD-ext II)

Unique Project (Investment) Identifier: 019-20-01-21-02-1032-00

Operated at
Brookhaven National Laboratory
Fermi National Accelerator Laboratory
Thomas Jefferson National Accelerator Facility

for the
U.S. Department of Energy
Office of Science
Offices of High Energy and Nuclear Physics

Version 1.1

April 8, 2015

PREPARED BY:
Robert D. Kennedy, FNAL

CONCURRENCE**:**

William N. Boroski
LQCD Contractor Project Manager

April 24, 2015
Date

LQCD-ext II Cyber Security Plan
Change Log

Revision No.	Description / Pages Affected	Effective Date
1.0	Adopt this document for LQCD-ext II from LQCD-ext	February 12, 2014

Table of Contents

1. SCOPE AND PURPOSE

This document has been prepared in accordance with guidance contained in DOE G 413.3-14, *Information Technology Project Guide*, which requires that a cyber security risk assessment be conducted in accordance with organizational cyber security plans (PCSP). The three U.S. Department of Energy (DOE) sites that will host the computing facilities for the SC Lattice Quantum Chromodynamics Computing Project Extension II (LQCD-ext II) are Brookhaven National Laboratory (BNL), Fermi National Accelerator Laboratory (FNAL), and Thomas Jefferson National Accelerator Facility (TJNAF).

2. CYBER SECURITY PLAN

The existing LQCD system of computing facilities is classified as a minor application contained in the general computing enclave at Fermilab and in the scientific computing enclaves at TJNAF and BNL. Security risk assessments, security controls, and contingency plans for the LQCD systems are documented in the security plans for each site, which are prepared in accordance with NIST Special Publication 800-18, Revision 1: *Guide for Developing Security Plans for Federal Information Systems.*

An annual security vulnerability assessment is performed for the LQCD minor application using scanning tools and documentation reviews, to identify those areas that are not covered by the general/scientific computing enclave cyber security plan. Potential vulnerabilities are identified and controls are put into place to mitigate these vulnerabilities. These vulnerabilities and controls are documented in risk assessment documents specific to each site.

Each host institution has appointed a site manager who is responsible for the operation of LQCD-ext II computing facilities at that particular site. These site managers are very experienced, having implemented and maintained security controls for the original LQCD project as well as the LQCD-ext project. Since the architecture of the systems planned for deployment and operation during LQCD-ext II will essentially remain the same throughout the project, the security controls in the aforementioned NIST 800 security plan document will apply.

All three sites, as are part of their respective computing enclaves, have been certified and accredited (C&A) with Authority to Operate as documented in the LQCD-ext II project's C&A Documentation. Given past experience, we anticipate that all three sites will continue to meet C&A requirements and that Authority to Operate will be maintained throughout the planned duration of the LQCD-ext II project.

No classified or sensitive data will be stored on the LQCD-ext II system. Therefore, the data sensitivity of data stored on the LQCD-ext II system or on attached data stores is classified as low as shown in the following table:

Table 1. Relative Importance of Protection Needs			
	HIGH (Critical Concern)	MEDIUM (Important Concern)	LOW (Minimum Concern)
Confidentiality			X
Integrity			X
Availability			X