Cyber Security Plan
for
Lattice QCD Research Program Extension III

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

Operated at
Brookhaven National Laboratory
Fermi National Accelerator Laboratory

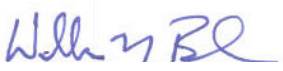
for the
U.S. Department of Energy
Office of Science and High Energy

Version 0

June 18, 2019

PREPARED BY:
Josephine Fazio, FNAL

CONCURRENCE:



William N. Boroski
LQCD Contractor Project Manager

July 3, 2019
Date

LQCD-ext III Cyber Security Plan
Change Log

Version No.	Description / Pages Affected	Effective Date
0.0	Updated to reflect LQCD-ext III operations model.	June 5, 2019

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 two U.S. Department of Energy (DOE) sites that will host the computing facilities for Lattice Quantum Chromodynamics Computing Research Program Extension III (hereafter LQCD) are Brookhaven National Laboratory (BNL) and Fermi National Accelerator Laboratory (FNAL).

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. 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.

At Brookhaven the IC, KNL, and Skylake clusters are part of the SDCC facility and their cybersecurity is governed by our subsystem security plan or inherits from the BNL site-level security plan.

Security risk assessments, security controls, and contingency plans are documented in the security plan for BNL and SDCC, which are prepared in accordance with NIST 800-53.
Ongoing security vulnerability assessments are performed for all SDCC service using scanning tools and other network monitoring utilities. Potential vulnerabilities are identified, and controls are put into place to mitigate these vulnerabilities. These vulnerabilities and controls are documented in the subsystem security plan.

Each host institution has appointed a site manager who is responsible for the operation of the LQCD 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 III program. Since the architecture of the systems planned for deployment and operation during LQCD-ext II will essentially remain the same throughout the program, the security controls in the aforementioned NIST 800 security plan document will apply.

The two sites that are part of their respective computing enclaves, have been certified and accredited (C&A) with Authority to Operate as documented in the LQCD Research Program C&A Documentation. Given past experience, we anticipate that both sites will continue to meet C&A requirements and that Authority to Operate will be maintained throughout the planned duration of the LQCD project.

No classified or sensitive data will be stored on the LQCD system. Therefore, the data sensitivity of data stored on the LQCD 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