DCPP Procedure CF2, Revision 8, "Computer Hardware, Software and Database Control"
(LAR Reference 49)

Computer Hardware, Software, and Database Control

08/16/11
Effective Date

QUALITY RELATED

Table of Contents

1. PROGRAM OVERVIEW

1.1 This Program Directive (PD) establishes overall policies and general requirements related to the quality and security of computer hardware, software, and database control processes for the plant. Because computer applications cover a variety of complex and diverse operational requirements, the appropriate quality assurance and information security requirements are determined on a system by system basis.

1.2 There are several considerations when establishing the level of quality and information security required for the development or procurement of any particular application. Quality or business critical applications may be developed under a quality assurance program within the company or with a vendor that meets plant requirements. A commercial grade application may be purchased and certified for its intended function at the plant. An application may be used to control plant systems and gather and process data from the power plant for use by plant staff. An application may run on a desktop alone or be shared by several users. In order to better serve the needs of the program, systems and applications are divided into the following classifications:

- Power plant applications and systems
- Business applications and systems
- Security applications and systems

2. APPLICABILITY

2.1 This Program Directive is applicable to all persons involved in the procurement, development, certification, or use of computer systems in the performance of activities related to the plant. This includes:

- Plant personnel
- Personnel matrixed to the plant from other company business units
- Personnel in other plant business units that are engaged in activities in support of the plant
- Contractor personnel who are engaged in activities in support of the plant

2.2 Although business, security, and power plant systems may have different processes and procedures to perform their tasks, this procedure applies to all business, security, and plant digital assets that are within the scope of the quality assurance or cyber security programs.[T35684/T36711]

3. DEFINITIONS

3.1 Certification: The documented acceptance that the computer system conforms to the specified requirements.

3.2 Computer Applications: The use of computer systems, both hardware and software, to serve a particular function, such as process control and monitoring, direct control of equipment, design/analysis calculations, display of information, data storage, etc.

3.3 Computer System: A functional unit, consisting of one or more computers and associated software that uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program; performs user-designated data manipulation, including arithmetic operations and logic operations.

3.4 Critical Application: An application that, if it were to fail, would impact safety, security, and emergency preparedness (SSEP) systems, the quality of operational or maintenance decisions, or result in significant financial loss.

3.5 Critical Digital Asset (CDA): A digital computer, communication system, or network that is a component of a critical system (this includes assets that perform SSEP functions; provide support to, protect, or provide a pathway to critical systems), or a support system asset whose failure or compromise as the result of a cyber attack would result in an adverse impact to a SSEP function.

3.6 Defensive Model: Documented definition or graphical representation of the graded approach which is used to classify the digital assets.

3.7 Defensive Strategy: Documented collection of technology, administrative processes and programmatic processes that ensure the appropriate level of security at each level in the defensive model.

3.8 Hardware: Physical equipment used to process, store, or transmit computer programs or data.

3.9 Incident Handling and Response Plan: An organized approach to addressing and managing the aftermath of an information security breach or cyber attack.

3.10 Life Cycle: The period of time beginning with computer system and/or application conception and ending with its retirement.

3.11 Quality Related: Refer to OM5, "Quality Assurance Program."

3.12 Software: Computer programs, procedures, and associated documentation and data pertaining to the operation of a computer system and/or application.

3.13 Software Quality Assurance (SQA) Plan: A plan for managing the lifecycle of software; SQA addresses the functional requirements, development, testing, maintenance, and retirement of software necessary to provide adequate confidence that the software conforms to established requirements. Implicit in this definition is the compatibility with the supporting hardware, firmware and operating systems.

4. PROGRAM OBJECTIVES AND REQUIREMENTS

4.1 Quality Assurance

4.1.1 The clear definition and implementation of appropriate quality assurance controls and documentation for computer applications should be provided.

> **NOTE:** It is recognized that computer usage ranges from simple aids entirely within the control of the user to complex computer systems that are relied upon without human intervention for the design, analysis, or operation of quality-related systems, structures, or components.

4.1.2 Degree of quality assurance control should be commensurate with the importance of the system and consequences of failure.

4.1.3 Implementing procedures associated with this PD should clearly define the:

a. Criteria for identifying and classifying computer systems

b. Quality assurance requirement based on established classification

4.1.4 Formal SQA plans should be provided for managing the life cycle of computer applications when required.[T35684]

4.1.5 Implementing procedures should ensure:

a. Only certified computer systems are used for critical applications that are relied upon without human evaluation or verification of the output.

b. Certified computer systems are used within the areas and the ranges of applicability specified in the SQA plan for each certified computer system.

c. Contracts for procurement or development of computer systems from contractors (e.g., vendors, service-bureaus, architect engineers, or consultants) contain the functional, technical, reporting, and quality requirements (i.e., elements of a software change package or equivalent) to ensure proper recourse if the purchased item is inferior.

4.2 Cyber Security

4.2.1 The clear definition and implementation of appropriate cyber security controls to effectively and efficiently manage cyber security issues for safety, security and emergency preparedness (SSEP) systems should be provided.

4.2.2 Critical digital assets should be assessed on an ongoing basis to characterize the cyber risk to the plant and appropriately mitigate unacceptable cyber weaknesses and vulnerabilities.

4.2.3 A comprehensive cyber security defensive strategy, to include a formalized incident handling and response plan, should be developed and maintained.

4.2.4 Cyber security should be integrated as a discipline within the engineering design and maintenance processes.

4.2.5 Processes should be provided to ensure Diablo Canyon Power Plant complies with cyber security-related regulatory requirements.

4.3 System Responsibilities

> **NOTE:** The establishment of ownership and responsibility for specific aspects of computer systems enhances accountability and delineates management and maintainability.

4.3.1 Specific objectives should ensure:

a. Responsibility for computer system development and ongoing maintenance is clearly assigned at a section manager level.

b. Appropriate plant organizations are responsible for data integrity. Organizations providing or inputting data are responsible for the correctness of the data. Access to systems shall be controlled as needed to prevent unauthorized changes.

c. Technical aspects of installation, maintenance, configuration management, and operation of applications using the mainframe or network are assigned to information technology.

d. The information technology department is consulted and concurs on questions of standardization, company (or business unit) strategic plans, current industry products, etc.

4.4 Managing Computer Resources

4.4.1 Coordination of plant computer systems should assess competing needs in light of realistic financial constraints. Specific objectives should:

a. Provide for a uniform process of evaluating and prioritizing computer system requests.

b. Provide coordination of responsibilities for computer system control activities.

c. Maximize the benefits of standardization within the plant and company.

4.4.2 Plant representatives should provide a forum for addressing the issues involved in managing computer related activities.

5. RESPONSIBILITIES

5.1 Engineering services vice president is responsible for:

5.1.1 Cyber security program.

5.1.2 Sponsoring of the cyber security program.

5.1.3 Designating a cyber security program manager.

5.2 Site services director is responsible for:

5.2.1 Designating a SQA program owner.

5.2.2 Sponsoring of the SQA program.

5.3 Station cyber security program manager is responsible for acting as a single point-of-contact for Diablo Canyon Power Plant cyber security issues with full responsibility and accountability for the cyber security program.

5.4 Engineering director is responsible for implementing the SQA program requirements for engineering controlled power plant applications and systems.

5.5 Security director is responsible for implementing the SQA program for security applications and systems.

5.6 Information technology manager is responsible for:

5.6.1 Implementing the SQA program for business applications and systems.

5.6.2 Ensuring the programs meet the requirements and needs of the site and they receive appropriate attention, support, and compliance.

5.7 Plant directors are responsible for:

5.7.1 Ensuring the use of appropriately controlled computer systems per CF2 procedures.

5.7.2 Ensuring adherence to the requirements of this PD for computer system procurement, development, and maintenance activities.

5.7.3 Ensuring adherence to SQA and cyber security requirements.

6. KEY IMPLEMENTING DOCUMENTS

6.1 Subjects Required to be Covered by IDAPs

6.1.1 Procuring, controlling, using, and maintaining computer systems that could affect plant safety systems or licensing commitments.

6.2 Subjects Required to be Covered by DLAPs

None

7. CLOSELY RELATED PROGRAMS

7.1 AD9, "Procurement Control"

7.1.1 Procurement control provides controls for specifying technical and quality requirements when procuring computer hardware, software, or computer systems.

7.2 CF3, "Design Control"

7.2.1 Design control provides controls on using computer systems for design work and provides controls for designing installed plant process control and monitoring systems.

7.3 CF4, "Modification Control"

7.3.1 Modification control controls changes to installed plant process control and monitoring systems and ensures conformance to the design bases.

7.4 OM11, "Security"

7.4.1 Security addresses the application of computer hardware, software, and databases. OM11, "Security" addresses security safeguards information related to these computer systems.

7.5 AD10, "Records"

7.5.1 Records address the requirements for maintaining records with computer systems.

8. RECORDS

None

9. REFERENCES

9.1 ANSI/IEEE Standard 610.12-1190, "Glossary of Software Engineering Terminology," December 10, 1990

9.2 ASME NQA-1-1997 Part 2.7, "Quality Assurance Requirements of Computer Software for Nuclear Facility Applications"

9.3 IEEE Std. 828-2005; IEEE Standard for Software Configuration Management Plans

9.4 IEEE Std. 1042 -1987; IEEE Guide to Software Configuration Management

9.5 INPO 86-024 (TS-407), "Software Controls for Plant Computers," Revision 1, December 1991

9.6 NEI 08-09, Rev. 6, April 2010 Cyber Security Plan for Nuclear Power Reactors

9.7 NRC Reg. Guide 1.169; Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

9.8 NUREG/CR-4640, August 1987, "Handbook of Software Quality Assurance Techniques Applicable to the Nuclear Industry"

9.9 QA Commitment: FSAR Chapter 17.3